Anti-Ransomware Capabilities Analysis

Ellis Research Institute

Authored by: Andrew C. Ellis, GSEC GCIA

Table of Contents

Overview

Ransomware presents a significant threat to organizations of all types and sizes[1]. Its ability to quickly render data and systems unusable can make its impact severe[2]. With the relative ease of execution and high return on investment when ransoms are paid, these types of attacks are only predicted to continue[3]. In most cases, a ransomware outbreak is not stealthy, as the obvious destruction of data is the goal intended by adversaries. These factors have led to increased discourse among cyber security vendors and experts on how best to deal with the threat of ransomware. When attempting to defend themselves against ransomware outbreaks, organizations can find a plethora of potential solutions to choose from. These solutions may all be effective; however, security teams have a finite set of resources with which they can implement capabilities. This presents the distinct need for a prioritized set of recommendations for protecting organizations against ransomware outbreaks.

This paper outlines the analysis of eight different recommended ransomware solutions in an attempt to present guidance on a combination of capabilities which can adequately protect organizations from the threat of ransomware. In order to identify salient combinations, the solutions are considered from two perspectives. The first, an idealistic view, ignores considerations such as budget and operational overhead in order to identify the "best" possible solution based on the pool of recommendations. The second perspective, a more realistic view, focuses on organizations with limited budgets, expertise, and personnel and aims to present a viable solution given these constraints.

The problem of identifying effective, compatible, and realistic solutions to cyber threats is not unique to ransomware. Cyber security teams are regularly required to define tactics and strategies for defending against a wide array of threats. By using ransomware as an example, this paper also tests and reviews various analysis methodologies which could be leveraged by organizations planning for other threats. These methodologies leverage multiple perspectives by drawing on publicly available guidance and data, input from subject matter experts, defense-in-depth principles, and a mixture of subjective and objective analysis techniques. Each of these analysis methodologies should be applicable to most security organizations.

A multiphase process was used to address the both purposes of this paper, identifying a prioritized set of anti-ransomware capabilities and providing a set of analysis techniques which can be applied to cyber security problems. This process began with defining the stages of a ransomware outbreak and creating a high level strategy which could be used as a framework for validating solutions. The analysis which followed drew on these definitions and compared the potential anti-ransomware capabilities to understand the strengths and weakness of each. A testing phase aligned the analysis results with both real world data and the anti-ransomware strategy defined in this paper in order to determine if the resulting solutions identified were effective. Finally, a review of the overall results was conducted in order to produce a salient anti-ransomware strategy and identify which analysis techniques, if any, were most effective.

Background

Ransomware is a specific type of malicious software designed primarily to destroy data or render systems unusable. Typically the goal of a ransomware outbreak is to generate profit for the bad actor[4] by requiring that the target provide payment in order to receive a recovery code or tool to restore data. In some instances, the destruction of the data itself is the primary goal and recovery options aren't provided or viable. In these cases, the destruction of data may be of ancillary purpose, such as to destroy evidence of other malicious activity or purely to render systems unusable to disrupt operations[5].

Ransomware is a common problem for organizations of all sizes and verticals. The impact of a wide-spread ransomware outbreak can be extremely damaging, resulting in the loss of data[6], revenue[7], or of customer trust[8]. Ransomware can spread extremely quickly, making preemptive planning and implementation of mitigating measures essential. A security team can find many recommendations to mitigate or prevent ransomware; however, the multitude of solutions can add to the complexity of solving the problem. These recommendations often are provided in a vacuum and do not include prioritization or considerations for real-world constraints. Organizations looking to defend against ransomware may be subject to budgetary or resource limitations, highlighting the need for defensive recommendations to include context for when to implement them.

Ransomware is a constant threat and is being leveraged by both opportunistic and targeted actors[9]. The Verizon Data Breach Investigations Report found that ransomware represented 39% of malware specific incidents in 2018[10] and 24% in 2019[11]. As organizations adapt to the threat of ransomware's destructive power, bad actors leveraging these techniques have begun to include other malicious capabilities which provide a foothold for future attacks[12] and to demand that organizations pay to not have their sensitive data released[13]. This evolution from basic ransomware attacks further highlights the need for organizations to take the threat seriously.

Analysis Methodology

In order to identify defensive strategies capable of defending against ransomware, the Ellis Research Institute used a multiphase methodology for reviewing capabilities and their combinations. This methodology involved understanding and defining the problem, conducting multiple types of analysis across the anti-ransomware capabilities, testing and reviewing the results, and drawing conclusions to produce anti-ransomware guidance and to develop an understanding of which analysis techniques were most useful. This methodology incorporated public information and data sources, commentary from subject matter experts, and multiple forms of analysis.

Phase 1: Defining the problem

The Ellis Research Institute began by defining ransomware using the Cyber Modeling Framework[14]. This model represented ransomware behavior through five generic steps which would occur during an outbreak. Each step was connected through a relational graph of assets, requirements, and generic vulnerabilities which would be exploited by ransomware throughout it's operation. This model outlined the progression from initial infection to encryption and lateral movement and provided a foundation for subsequent analysis.

A high level anti-ransomware strategy, which identified the key problems presented by ransomware, was also created and paired with high level policies which govern critical aspects of prevention and mitigation. These policies were used to guide analysis and to subject each potential solution set to additional scrutiny. This strategy allowed for the determining if solutions would be successful in achieving a robust anti-ransomware defensive posture.

Phase 2: Analysis

Five different analysis techniques were leveraged to identify potential combinations of capabilities, or "solution sets", which would provide a defense against ransomware. These analysis techniques were selected to provide multiple viewpoints into the effectiveness of potential solutions and included subjective, qualitative, and quantitative analysis.

Three analysis techniques were based on guidance provided by subject matter experts in the form of public recommendations, commentary, and a ransomware focused survey. These techniques drew on the combined expertise of cyber security and information technology professionals who deal with ransomware, either directly or indirectly, on a regular basis. Public recommendations were collected from seven different reputable sources who have produced lists of anti-ransomware capabilities. In addition to using recommendations made by these groups as the core suite of anti-ransomware capabilities reviewed in this paper, analysis was conducted to identify capabilities which were recommended by multiple parties. Subject matter expert commentary was sourced from five experts and allowed for free-form guidance from a variety of perspectives. A survey was conducted involving sixteen technology experts which focused on ranking potential solutions as well as collecting information on the cost, deployment, and operational overhead required to support each solution. These three techniques were primarily subjective in their review of potential capabilities and were designed to offset implicit biases of this paper's author and to ensure that multiple viewpoints were considered.

Two analysis techniques were based on a more objective quantification of the selected potential capabilities. A review was conducted using the Ellis Research Institute's Cyber Modeling Framework which focused on the overlapping coverage provided by combinations of capabilities. Leveraging the model created in the definition phase, capabilities were mapped to the aspects of ransomware's execution which they prevented or mitigated. The resulting enhanced model was then used to identify combinations of solutions which provided reenforcing capabilities. To supplement this relational analysis with a more direct review of each capability's effectiveness, a Failure Mode and Effects Analysis[15] (FMEA) was conducted. This analysis considered each capability's ability to reduce the impact and occurrence or increase the detectability of each phase of a ransomware outbreak, as defined in the model. The combination of these two techniques allowed for a more objective analysis to be conducted, resulting in the identification of effective capabilities.

Phase 3: Review and testing

The results of each analysis technique produced one or more solution sets of capabilities, which represent potential defensive suites focused against ransomware. These solution sets are based on high level, and in some cases, very focused analysis. In order to reduce the list of solution sets to a salient listing of actual solutions, the Ellis Research Institute used two methods to test and review the actual effectiveness of these solution sets – comparisons with real world data and alignment against the anti-ransomware strategy. The results of this testing allowed for both the identification of viable solutions sets and provided insight into which analysis techniques were most effective.

To effectively test the various solution sets, analysis reports for real world and well understand ransomware variants were collected. Findings included in publicly available analysis reports for each variant were reviewed and used to determine which capabilities would have prevented each variant. This mapping was then compared to the solution sets identified in phase 2, providing a score based on the number mitigations per ransomware variant. Solution sets were then ranked leveraging these scores to determine which would be most effective in practice.

Solution sets were also compared against the anti-ransomware strategy to ensure they adhered to the guiding principles identified as core components of any effective strategy. These criteria required that any solution 1) provided defenses which could operate at the speed of ransomware, 2) included defenses which overlapped and covered the entire ransomware chain of execution, and 3) allowed for recovery in the event that an outbreak bypassed other defenses. By ensuring that a solution set included all of these features, organizations can have confidence that it will be resilient to emergent ransomware variants and not only those included in the real world data review.

Phase 1 – Definition

Anti-Ransomware Strategy

In order to determine if any set of capabilities constitutes an effective defense against ransomware, it is important define a strategy which can be used to validate that the solution actually solves the problem that ransomware presents. At its core, a ransomware outbreaks is based on two primary factors – the speed at which it spreads and its destructive nature. These aspects make defending against ransomware a difficult task. While an outbreak is highly detectable, manual responses are typically too slow to effectively mitigate the damage. Additionally, like any other malicious activity, bad actors have a wide variety of tactics at their disposal to infect systems, spread throughout environments, and destroy data. This further complicates any potential preventative capabilities as it is impossible to protect against all possible exploits.

In order to offset these key concerns, an anti-ransomware strategy must be based on defensive capabilities which are automated or preemptive and are supported by a robust ability to recover from the impact. Automated and preemptive capabilities allow for defenses to keep up with the fast paced nature of ransomware spreading throughout an environment, effectively limiting the scale of the impact. Recovery techniques support prevention by allowing affected organizations the ability to roll back any damage caused by ransomware which bypasses defenses. Furthermore, with the wide ranging set of tactics a bad actor can employ, ensuring that defensive capabilities exist throughout the chain of events allows for more potential for them to be effective; rather than relying on a singular defense.

Figure 1 – Anti-Ransomware Strategy Definition

Key Problems	**Defensive Principles**
✗ Ransomware is fast moving and difficult to contain	✔ Reduce impact through automated or preemptive defenses
✗ Ransomware is highly destructive	✔ Ability to recover destroyed data
✗ Ransomware makes use of a variety of tactics	✔ Overlapping defenses across the entire chain of events

This definition of the problem and the principles which should followed can be used to judge solution sets produced by the subsequent analysis. Any solution set which does not provide both automated or preemptive defenses and recovery capabilities will not appropriately protect an organization against the threat of ransomware outbreaks. Therefore, solution sets generated throughout the analysis phase can be ranked based on their adherence to these criteria.

In addition to these capability-specific criteria, any strategy produced must consider real world budgetary and resource constraints to be practically applicable. As such, any solution sets generated throughout this paper will be limited to a total of three capabilities per set. This allows for flexibility in achieving the defensive principles laid out in the core strategy, without creating solutions which are impractical for organizations looking for guidance.

Ransomware Model

The Ellis Research Institute created a generic model of the behavior of ransomware leveraging the Cyber Modeling Framework. This framework, created by the Ellis Research Institute, was designed to allow for the abstraction of events and a representation environments in order to understand the requirement-cause-effect chains present in multistage attacks. The ransomware model simplifies the specifics of assets, vulnerabilities, and objectives into set of interconnected steps which can be reviewed to analyze the impact of various defensive and responsive capabilities. The high-level nature of this model makes it suitable for discussing ransomware's effects on organizations of all sizes and types.

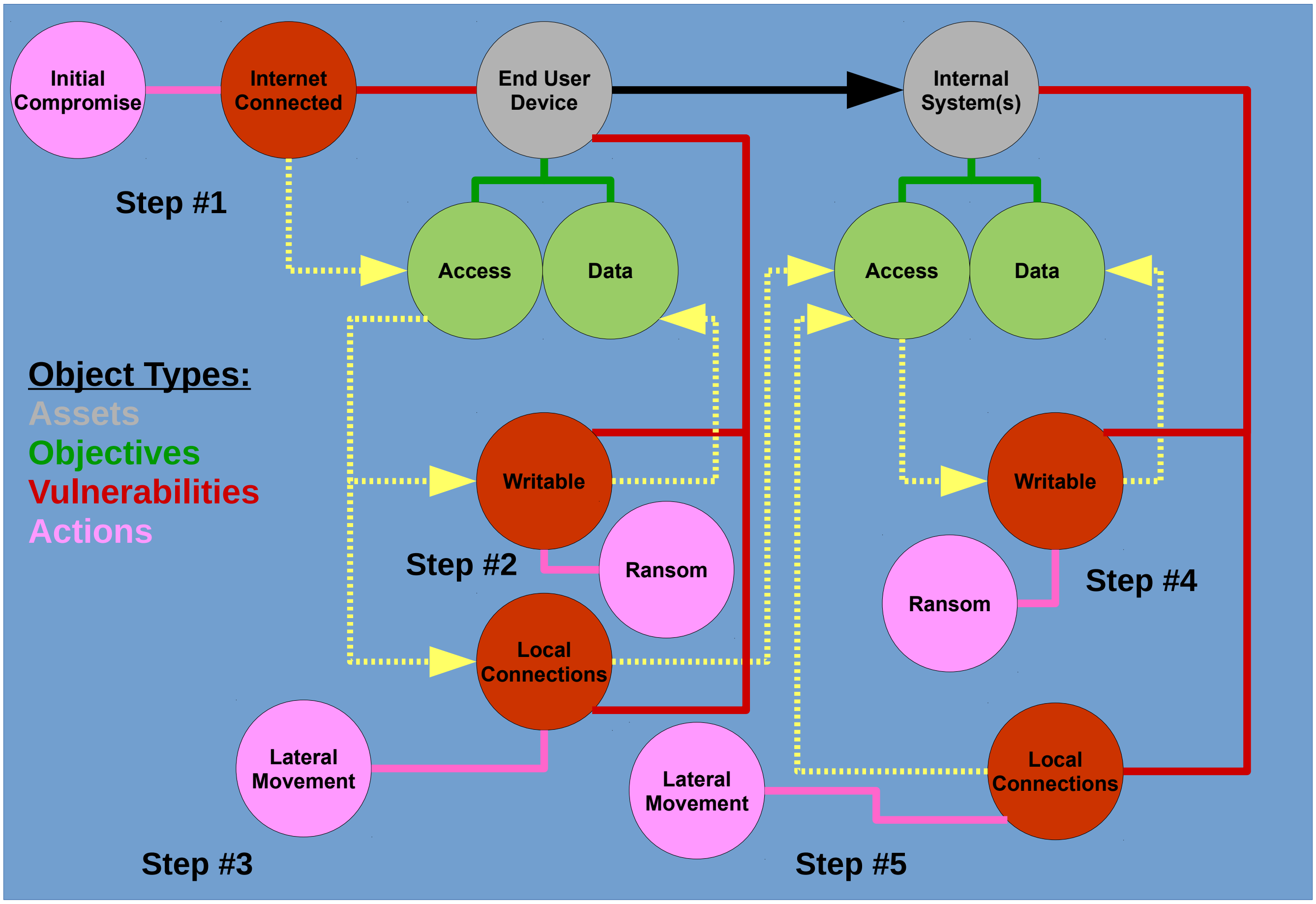
In order to develop the model, a generic ransomware process first needs to be defined. A ransomware outbreak begins with the initial infection of a host (step 1.) This host is then subjected to encryption (step 2) and used to laterally move to other connected hosts (step 3.) Each subsequent host is then also encrypted (step 4) and used to continue spreading (step 5.) In most cases, steps 4 and 5 will be repeated until all accessible and vulnerable hosts have been encrypted and used as a pivot point. Using these five steps, a model was built to represent a ransomware outbreak.

The model is based on two primary assets – the "end user device", or initial point of compromise, and "internal systems", other accessible devices. The end user device represents the source of the initial infection, often an employee controlled device. The internal systems represent all other devices, including other end user devices, which are contained within the environment. Objectives of "access", the ability for ransomware to execute, and "data" the ability for ransomware to interact with files, exist for both asset types.

Both asset types present vulnerabilities in the form of "local connections", allowing for lateral movement, and "writable" file access, allowing for the destruction and subsequent ransom of data. These vulnerabilities both rely upon the ransomware having already achieved the access objective, as neither can be accomplished without the ability to preform actions on the affected host. Local connections, when successfully exploited, allows the ransomware to gain access to other systems and to spread throughout the environment. In the case of both the end user device as well as the internal systems, this access is to other internal systems represents the spread throughout an environment. The writable file access only affects the "data" objective associated with the asset itself.

The end user asset presents a third, unique vulnerability in the form of being "internet connected" which allows for the initial infection. The specific method of infection, whether it be via malicious email, drive-by download, opened ports, or some other factor, are all exposed due to this generalized vulnerability. It is important to note that internal systems could also be internet connected. As this model was built as a generalized behavior chain, should one of those systems be the initially compromised host – those hosts would then take the place of the end user device, regardless of if they actually were controlled by an end user. A visual representation of this model is provided below:

Figure 2 – Cyber Modeling Framework representation of a ransomware outbreak



Phase 2 – Analysis

Recommendations Collection

For many cyber threats, including ransomware, it is not difficult to amass a large number of recommendations provided by vendors, experts, government agencies, academic institutions, and other resources. These recommendations are rooted in common sense and typically draw from the direct experience of the authors.

The Ellis Research Institute gathered recommendations from seven of these types of sources, including two government agencies[16][17], three technology vendors[18][19][20], one academic institution[21], and one publisher focused on technology[22]. The analysis conducted on these recommendations consisted purely of treating each source as a voting entity and ranking solutions based on the number of votes they accrued. The top eight solutions were used as potential capabilities throughout this paper. The results of this voting were also used as an analysis technique to produce a solution set based on publicly available guidance. Definitions of each capability reviewed in this paper can be found in Appendix A.

Figure 3 – Anti-ransomware recommendations matrix

	US-CERT	FBI	Trend Micro	Norton	Microsoft	Carnegie Mellon	Wired magazine	Total
Patching	Yes	Yes	Yes	Yes	Yes	Yes	Yes	**7**
Backups	Yes	Yes	Yes	Yes	Yes	Yes	Yes	**7**
Security Awareness Training	Yes	Yes	Yes	Yes	No	Yes	Yes	**6**
Anti-virus	Yes	Yes	No	Yes	No	Yes	Yes	**5**
Email Security Suites	Yes	Yes	No	No	No	Yes	No	**3**
Role Based Access Controls (RBAC)	No	Yes	No	No	No	Yes	Yes	**3**
Application Whitelisting	No	Yes	Yes	No	No	No	Yes	**3**
Firewalls	Yes	Yes	No	No	No	Yes	No	**3**
Total	**6**	**8**	**4**	**4**	**2**	**7**	**6**	

All seven sources recommended both backups and patching as critical anti-ransomware capabilities. Backups, if well maintained and isolated, represent the most effective response to ransomware as they can offer total recovery. Patches were also ubiquitously cited as important, as many ransomware variants make use of well-known vulnerabilities which software and operating system providers release updates to address. Security awareness training and anti-virus took third and fourth place, respectively, with minor disagreements among the sources as to which would be more effective. While many attributed the need for security awareness training, as many ransomware outbreaks take advantage of phishing or mal-spam, it was also noted that most anti-virus products offer anti-ransomware signatures to prevent common methods of data destruction, alongside capabilities which prevent initial infections and lateral movement. The remaining solutions varied depending on the mindset of the source. Based purely on these recommendations the most highly recommended solutions are backups, patches, and security awareness training.

The Ellis Research Institute notes that of the seven sources, four recommended 75% or more of the potential solutions considered in this paper. This highlights the problem for organizations looking to base their anti-ransomware program, or other security strategies, on public guidance. While implementing all of these capabilities would create a robust defensive posture, there are many considerations which make the "kitchen sink" approach infeasible – such as budgetary limitations or the complexity of implementation. This illustrates the need for a methodology to produce a more focused set of recommendations which provides the largest return on investment.

Recommendation's Solution Set:

✔ Backups, patches, and security awareness training

Model Analysis

Leveraging the model developed during the first phase of this project, the Ellis Research Institute categorized each of the eight solutions based on which steps in the ransomware process they were likely to prevent or mitigate. The results were then applied to the model in order to identify solutions which provided a depth of defense. Combinations of solutions were generated which met three primary criteria. First, any resulting solution set was required to address all steps in the ransomware process. Second, any resulting solution set was required to provide at least two unique capabilities for each step in the ransomware process, ensuring that no single point of failure existed. Third, solution sets which met these criteria were then limited based on the number of unique solutions which comprised them to identify sets with the minimum number of discrete components.

This analysis does not take into account the actual effectiveness nor the operational overhead for each solution. Instead, the analysis purely focuses on overall coverage to identify chains of solutions which can then be used for evaluating other solution sets. In the table below, each solution is listed along with the stages it will impact. These are classified as "Yes" where an impact to ransomware's operation is present.

Figure 4 – Solution alignment with ransomware stages

Solution	Malware Delivery	Lateral Movement	Ransom
Patches	Yes	Yes	No
Backups	No	No	Yes
Security Awareness	Yes	No	No
RBAC	No	Yes	Yes
Email Security Suites	Yes	No	No
Anti-virus	Yes	Yes	Yes
Application Whitelisting	Yes	Yes	No
Firewalls	Yes	Yes	No

With a focus on finding overlapping solutions for all stages, the limiting factor for each chain of security capabilities are those which address the ransom stage. Only three capabilities have the ability to prevent or mitigate the operations which ransomware uses to destroy data. These capabilities are anti-virus and role based access controls (RBAC), which address the issue by halting or limiting the spread of ransomware, and backups, which allows for the recovery from ransomware through copies of the data. In order for a solution set to properly implement defense in depth, it must include at least two of these capabilities.

Leveraging the table above along with a script which combined solutions, chains were produced which ensured that two or more capabilities were present for each stage of a ransomware outbreak. The shortest chains were then identified as potential solution sets. The result of this produced the following eight chains, each containing three unique solutions:

Figure 5 – Cyber Modeling Framework solution chains

Chain	Delivery	Lateral Movement	Ransom
Anti-virus, backups, application whitelisting	2	2	2
Anti-virus, backups, firewall	2	2	2
Anti-virus, backups, patches	2	2	2
Anti-virus, RBAC, application whitelisting	2	3	2
Anti-virus, RBAC, email security suites	2	2	2
Anti-virus, RBAC, firewalls	2	3	2
Anti-virus, RBAC, patches	2	3	2
Anti-virus, RBAC, security awareness training	2	2	2

Further categorization of the solutions was conducted to identify the percentage of solutions in which each solution appeared.

Figure 6 – Anti-ransomware solutions by solution set

Solution	Count	Percent of chains
Anti-virus	8	100%
RBAC	5	62.5%
Backups	3	37.5%
Firewall	2	25%
Application whitelisting	2	25%
Patches	2	25%
Email security suites	1	12.5%
Security awareness training	1	12.5%

Due to it’s ability to handle all three stages of a ransomware outbreak, anti-virus was identified as an essential component to any anti-ransomware strategy. While specially crafted ransomware may be able to defeat an anti-virus across all three stages, anti-virus provides the widest coverage of any single capability.

With protection against the ransom stage being our primary limiter, the determination of which chains listed above provide the best benefit for an organization comes down primarily to a decision between RBAC and backups as the supplemental capability. If backups are chosen, then patching, firewalls, and application whitelisting are the only solutions which completes the chain without additional “links.” If RBAC is chosen, then multiple options exist to round out capabilities – all of which focus on preventing the initial delivery of ransomware to the environment.

Without reviewing the effectiveness or overhead inherent to each solution, these chains only represent a set of options – not direct guidance. Subsequent analysis conducted in this paper will address reviewing each solution in more depth, to determine which combination will yield the most effective result.

Cyber Modeling Framework Solution Sets:

✔ Anti-virus, backups, application whitelisting
✔ Anti-virus, backups, firewalls
✔ Anti-virus, backups, patches
✔ Anti-virus, RBAC, application whitelisting
✔ Anti-virus, RBAC, firewalls
✔ Anti-virus, RBAC, patches
✔ Anti-virus, RBAC, email security suites
✔ Anti-virus, RBAC, security awareness training

Failure Mode and Effects Analysis

The Ellis Research Institute conducted a Failure Mode and Effects Analysis (FMEA) of all eight potential solutions to identify their relative strengths in the areas of prevention (reduction of occurrence), mitigation (reduction of severity), and identification (increase in detection.) This FMEA drew upon the steps defined in the ransomware model and the alignment of solutions with each step.

Each step in the ransomware process was assigned initial scores for severity, occurrence, and detection based on a scenario where no existing security controls were in place. The severity was dictated by the scope of the impact (number of effected elements) and the ability for an organization to recover from the impact. The occurrence was based on the likelihood and ease by which ransomware would be able to accomplish the step, with each step increasing the difficulty due to requiring the previous steps be successful. The detectability was based on the probability of detection and the point at which the activity would be detected. Using these definitions, each capability was then reviewed to identify changes to these scores, if the capability was implemented. Scales for each of these values are provided in Appendix D.

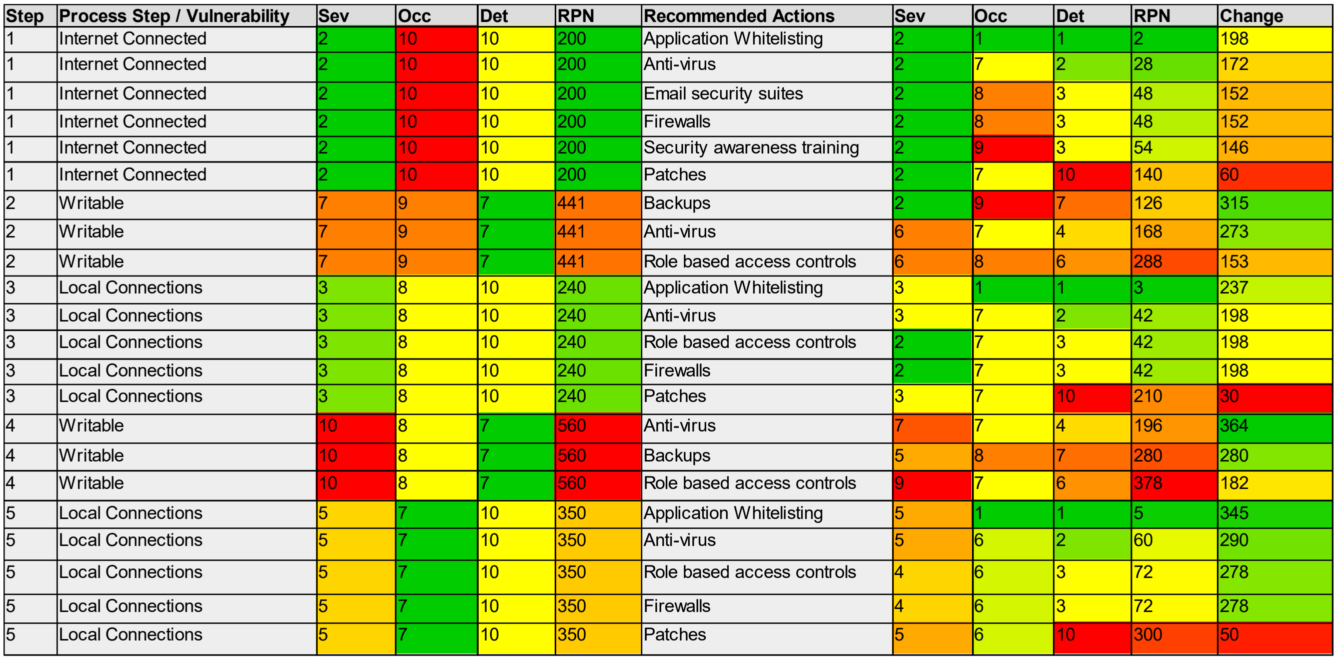
The results of these scores were then reviewed from five perspectives to identify solution sets which would provide the best defense against ransomware. Each review process used different criteria to identify the “best” solutions. First, each capability was reviewed for their overall impact to the risk prioritization number (RPN) scores for the problem to identify sets which provided the greatest quantitative benefits. Second, each capability was reviewed for the number of steps which they impacted to identify which sets provided the greatest depth of benefits. Third, each capability was reviewed for the largest total change in severity, occurrence, and detection to identify sets which resulted in the largest change in metrics. Forth, the capabilities were reviewed for the largest, lower limit change to identify sets which resulted in the strongest “weak link.” Finally, each capability was reviewed for the best solution for each step in the ransomware process to identify the sets which resulted in the most overall resilience to the ransomware process. While scores used are subjective, efforts have been made to normalize each component of the FMEA in order to provide direct comparisons.

For each stage, applicable capabilities are listed as the “recommended action”, and each score is adjusted based on the effects of the specific capability. This analysis was conducted to gain an understanding of the potential effectiveness of each capability and provides the ability to directly compare solutions on both a per-stage and overall basis. The change or “delta” between base RPN and modified RPN illustrates the overall difference in impact.

This analysis does not take into account any operational overhead, costs, or resources required to implement the strategies. These are important considerations and are a focus of the “Survey” review section of this paper; however, it is equally important to understand which capabilities provide the most benefits.

Below is an abbreviated FMEA table which shows each stage and the solutions which apply. A full view of the FMEA table is available in Appendix E.

Figure 7 – Abbreviated Failure Mode and Effects Analysis table

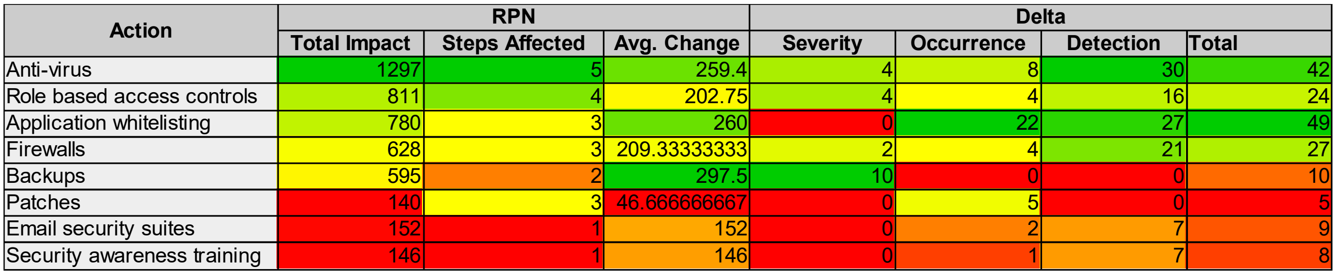


Step	Process Step / Vulnerability	Sev	Occ	Det	RPN	Recommended Actions	Sev	Occ	Det	RPN	Change
1	Internet Connected	2	10	10	200	Application Whitelisting	2	1	1	2	198
1	Internet Connected	2	10	10	200	Anti-virus	2	7	2	28	172
1	Internet Connected	2	10	10	200	Email security suites	2	8	3	48	152
1	Internet Connected	2	10	10	200	Firewalls	2	8	3	48	152
1	Internet Connected	2	10	10	200	Security awareness training	2	9	3	54	146
1	Internet Connected	2	10	10	200	Patches	2	7	10	140	60
2	Writable	7	9	7	441	Backups	2	9	7	126	315
2	Writable	7	9	7	441	Anti-virus	6	7	4	168	273
2	Writable	7	9	7	441	Role based access controls	6	8	6	288	153
3	Local Connections	3	8	10	240	Application Whitelisting	3	1	1	3	237
3	Local Connections	3	8	10	240	Anti-virus	3	7	2	42	198
3	Local Connections	3	8	10	240	Role based access controls	2	7	3	42	198
3	Local Connections	3	8	10	240	Firewalls	2	7	3	42	198
3	Local Connections	3	8	10	240	Patches	3	7	10	210	30
4	Writable	10	8	7	560	Anti-virus	7	7	4	196	364
4	Writable	10	8	7	560	Backups	5	8	7	280	280
4	Writable	10	8	7	560	Role based access controls	9	7	6	378	182
5	Local Connections	5	7	10	350	Application Whitelisting	5	1	1	5	345
5	Local Connections	5	7	10	350	Anti-virus	5	6	2	60	290
5	Local Connections	5	7	10	350	Role based access controls	4	6	3	72	278
5	Local Connections	5	7	10	350	Firewalls	4	6	3	72	278
5	Local Connections	5	7	10	350	Patches	5	6	10	300	50

The table above outlines the FMEA conducted for each step. This table shows that the highest impact failure mode is that of the ransom (writable) steps, with step 2 causing less impact than step 4, due to the number of the devices affected. Each of the solutions presented affect the severity, occurrence, and detectability of the ransomware stages in different ways, with some affecting all three and others affecting only a subset. The color coding on the modified RPN column clearly shows a divergence in the original score for each stage.

The results of this analysis were aggregated by recommendation and the total impact (sum of all RPN changes), total impacted steps (count of process steps affected), and changes in each FMEA metric were calculated. These scores were accumulated to understand the overall impact of each solution across all stages, and are outlined on the next page:

Figure 8 – Failure Mode and Effects Analysis scoring table



Action	RPN			Delta			
	Total Impact	Steps Affected	Avg. Change	Severity	Occurrence	Detection	Total
Anti-virus	1297	5	259.4	4	8	30	42
Role based access controls	811	4	202.75	4	4	16	24
Application whitelisting	780	3	260	0	22	27	49
Firewalls	628	3	209.33333333	2	4	21	27
Backups	595	2	297.5	10	0	0	10
Patches	140	3	46.666666667	0	5	0	5
Email security suites	152	1	152	0	2	7	9
Security awareness training	146	1	146	0	1	7	8

This table, organized by total impact, shows anti-virus as the solution with the largest impact, primarily due to the increase in detectability. Anti-virus is the only solution which affects all five steps, giving it more opportunity to present a meaningful change. Role-based access controls and application whitelisting rank second and third respectively, and also provide a significant benefit when evaluating the overall RPN change. Role based access controls provide this primarily by affected four out of five ransomware steps, whereas application whitelisting provides this primarily from the reduction in occurrence while also increasing detectability. Patches, email security suites, and security awareness training represent the lowest relative value in preventing ransomware, due to their limited scope. Patches only reduce the potential for occurrence at across three of five steps and email security suites and security awareness training only affect the first step (initial infection) of a ransomware outbreak. While ranking fifth, backups provide the most significant reduction in severity as it is the only capability with the ability to remediate the effects of ransomware's encryption steps.

When reviewing the results of this FMEA, five different interpretations of the data were used to determine ideal combinations of capabilities. These interpretations are:

- Overall RPN impact – an analysis of which solutions reduce the total RPN by the greatest amount
- Number of steps affected – an analysis of which solutions impact the most aspects of ransomware. This is partially redundant with the model analysis's focus on coverage
- Largest total delta – an analysis of the overall changes in the severity, occurrence, and detection values for each stage. This is different from "overall RPN impact" as it looks at stand-alone changes rather than the computed change
- Largest lower limit delta – an analysis of the overall changes in the severity, occurrence, and detection values for each step with an emphasis on ensuring the strongest "weak link"
- Best solution for each step – an analysis of which capability provides the largest impact on specific step of the ransomware process

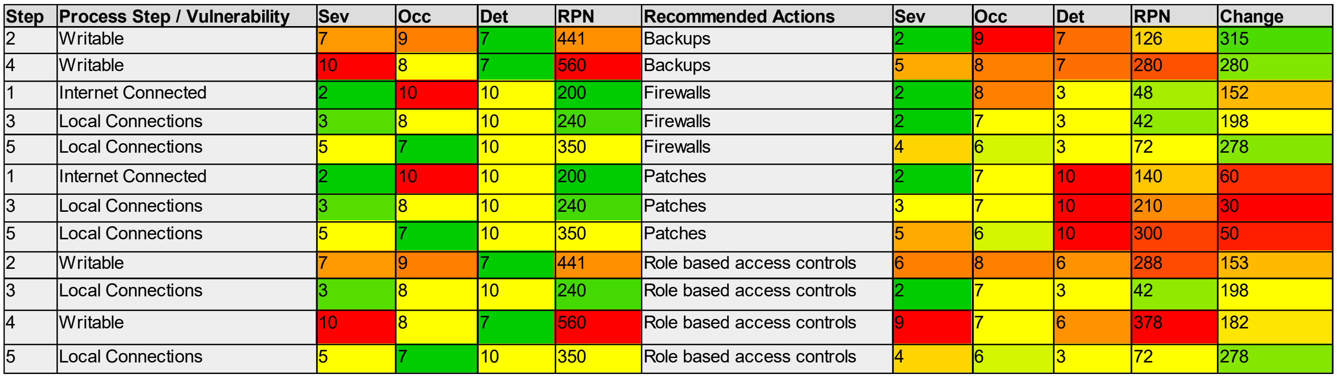
Figure 9 – Solutions by analysis type

	Anti-virus	RBAC	App. Whitelist	Firewall	Patches	Backups
Overall RPN impact	Yes	Yes	Yes	No	No	No
Stages affected	Yes	Yes	Yes*	Yes*	Yes*	No
Largest delta	Yes	No	Yes	Yes	No	No
Most even delta	Yes	No	Yes	No	No	Yes
Best stage solution	Yes	No	Yes	No	No	Yes
Total	**5**	**2**	**5**	**2**	**1**	**2**

** Application whitelisting, firewalls, and patches were tied, affecting three out of five stages*

When reviewing the results of these different approaches, the anti-virus and application whitelisting solutions are clear front runners – appearing in all five solution sets. The remaining four solutions represent variations which can be chosen based on an organizations needs or capabilities. A sub-table of the these solutions is provided below:

Figure 10 – Firewalls, patches, backups, and role-based access controls comparison



Step	Process Step / Vulnerability	Sev	Occ	Det	RPN	Recommended Actions	Sev	Occ	Det	RPN	Change
2	Writable	7	9	7	441	Backups	2	9	7	126	315
4	Writable	10	8	7	560	Backups	5	8	7	280	280
1	Internet Connected	2	10	10	200	Firewalls	2	8	3	48	152
3	Local Connections	3	8	10	240	Firewalls	2	7	3	42	198
5	Local Connections	5	7	10	350	Firewalls	4	6	3	72	278
1	Internet Connected	2	10	10	200	Patches	2	7	10	140	60
3	Local Connections	3	8	10	240	Patches	3	7	10	210	30
5	Local Connections	5	7	10	350	Patches	5	6	10	300	50
2	Writable	7	9	7	441	Role based access controls	6	8	6	288	153
3	Local Connections	3	8	10	240	Role based access controls	2	7	3	42	198
4	Writable	10	8	7	560	Role based access controls	9	7	6	378	182
5	Local Connections	5	7	10	350	Role based access controls	4	6	3	72	278

The variation between each of the possible solution sets is primarily seen in the type and focus of their effects. Backups, the only solution to provide change in the severity of the writable step, reduce the impact of a ransomware outbreak. Firewalls primarily increase the detectability of a ransomware as it enters and traverses the environment whereas patches provide a reduction in the occurrence of ransomware in these same steps. Role based access controls act as a middle ground, affecting every step except the initial infection and provide a reduction to both impact and occurrence, while also increasing detection, albeit by less than any of the more focused solutions. Patches limit the potential initial infection and lateral movement, by reducing the overall attack surface. The choice between these capabilities is most likely to come down to which supplemental solution an organization can most easily implement or which provides benefits missing in other areas of their security program.

Failure Mode and Effects Analysis Solution Sets:

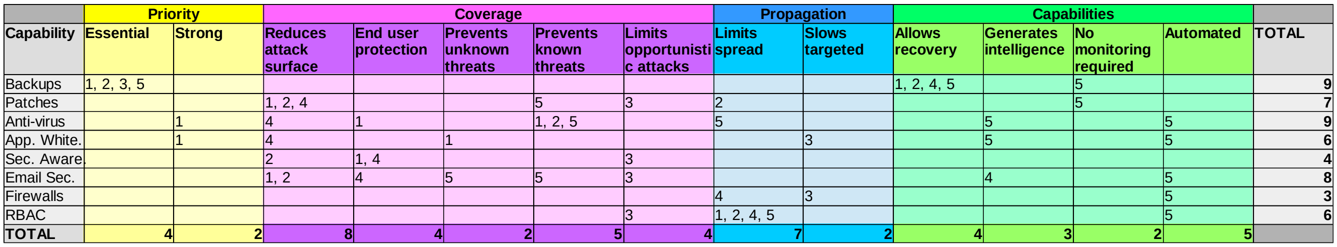
✔ Anti-virus, application whitelisting, backups (weakest link, best stage)
✔ Anti-virus, application whitelisting, RBAC (RPN, stages affected)
✔ Anti-virus, application whitelisting, firewalls (largest delta, stages affected)
✔ Anti-virus, application whitelisting, patches (stages affected)

Subject Matter Expert Commentary

In order to review the more subjective elements of each anti-ransomware capability, the Ellis Research Institute collected commentary from cyber security experts to gain additional insight into each potential solution. Five cyber security experts, including this paper's author, reviewed the eight recommended capabilities to provide additional, free-form thoughts regarding their effectiveness and implementations. These experts had a diverse background including expertise in offensive and defensive operations, threat intelligence, platform and infrastructure security, trusted advisory, and cyber security consulting. Responses were solicited with limited guidance on format or composition, to allow experts to address the request in their native, problem solving mindsets.

A listing of the experts involved is provided in Appendix B and each expert was provided with the same request for commentary. This method of review was designed to simulate the types of commentary generated during a "conference room" or "email thread" version of capabilities review. Each expert's commentary was reviewed by the author, grouped by strengths and weakness, normalized, and categorized. Each normalized topic was then attributed "votes" based on the experts who brought it up in their response. In an effort to keep responses anonymous each expert was assigned an "expert ID" which is listed in the table below to identify how each expert voted. The request for commentary and experts' responses are provided in Appendix C.

Figure 11 – Benefits identified by subject matter experts



	Priority		Coverage					Propagation		Capabilities				
Capability	**Essential**	**Strong**	**Reduces attack surface**	**End user protection**	**Prevents unknown threats**	**Prevents known threats**	**Limits opportunistic attacks**	**Limits spread**	**Slows targeted**	**Allows recovery**	**Generates intelligence**	**No monitoring required**	**Automated**	**TOTAL**
Backups	1, 2, 3, 5									1, 2, 4, 5		5		**9**
Patches			1, 2, 4			5	3	2				5		**7**
Anti-virus		1	4	1		1, 2, 5		5			5		5	**9**
App. White.		1	4		1				3		5		5	**6**
Sec. Aware.			2	1, 4			3							**4**
Email Sec.			1, 2	4	5	5	3				4		5	**8**
Firewalls								4	3				5	**3**
RBAC							3	1, 2, 4, 5					5	**6**
TOTAL	**4**	**2**	**8**	**4**	**2**	**5**	**4**	**7**	**2**	**4**	**3**	**2**	**5**	

Figure 12 – Limitations identified by subject matter experts

	Limitations				Implementation			Bypassable			Operations			
Capability	**Does not prevent**	**Known threats only**	**Limited number of protected vectors**	**No post infection impact**	**Difficult to implement**	**Training is hard**	**Requires other solutions**	**Exclusion lists**	**Required connectivity**	**Can be bypassed**	**Overhead**	**Shadow IT**	**Usability issues**	**TOTAL**
Backups	1, 2, 5				2						4, 5			**6**
Patches		5					2				4, 5			**4**
Anti-virus		1, 2, 4, 5						2			4			**6**
App White										2	4, 5	4	1, 5	**6**
Sec. Aware.				5		1, 2, 4, 5				2				**6**
Email Sec.			1	5		4				2, 4	5			**6**
Firewalls			1, 2		1			2	5		4			**6**
RBAC					1			2	5		4, 5			**5**
TOTAL	**3**	**5**	**3**	**2**	**3**	**5**	**1**	**3**	**2**	**4**	**11**	**1**	**2**	

These results were then analyzed, leveraging three different methods:

- Quantitative assessment of the voting scores
- Subjective assessment based on solutions identified by experts as critical or high priority
- Qualitative assessment based on aligning the categories cited by experts against the anti-ransomware strategy

The quantitative analysis of the voting "scores" was conducted by tallying the number of experts who discussed each topic and then subtracting the identified negative aspects from the positive aspects. The resulting score represents an unweighted confidence in each potential solution. This analysis was conducted from a purely empirical standpoint and is influenced by the lack of uniformity in the respondents' commentary. While the tallies for each strength ranged from three to nine, the tallies for the weakness were more tightly grouped ranging only from four to six. After computing these scores the solutions were ranked based on score (descending), strengths (ascending), and weaknesses (descending.) The results are detailed in the following table.

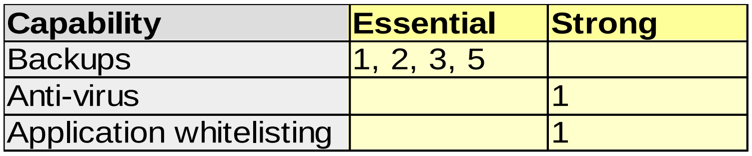
Figure 13 – Subject matter expert scores

Capability	**Strengths**	**Weaknesses**	**Score**
Anti-virus	9	6	3
Backups	9	6	3
Patches	7	4	3
Email security suites	8	6	2
RBAC	6	5	1
Application whitelisting	6	6	0
Security awareness training	4	6	-2
Firewalls	3	6	-3

Based these scores and continuing with the goal of selecting solution sets of three capabilities, the score-based analysis led to experts identifying anti-virus, backups, and patches as the optimal solution.

The subjective analysis of the commentary was based on cases where experts specifically identified "essential" or "strong" solutions. Throughout their responses, four of the five experts specifically identified backups as being essential, and one expert additionally listed anti-virus and application whitelisting as a strong solution. The following table shows the three solutions which were identified and which subject matter experts referenced them.

Figure 14 – Subject matter expert high priority solutions



Capability	Essential	Strong
Backups	1, 2, 3, 5	
Anti-virus		1
Application whitelisting		1

As only three solutions were specifically called out by experts, these do not require ranking and produce the solution set which contains backups, anti-virus, and application whitelisting.

Finally, a qualitative approach was taken to the attributes the experts identified and by aligning them to the anti-ransomware strategy. The strategy required that solution sets 1) be automated or not require human interaction, 2) have the ability to recover from damage caused by ransomware, and 3) be composed of capabilities which overlap to provide defense-in-depth. This analysis was conducted by ignoring the number of votes, and instead simply looking at the attributes of each capability called out by the experts. Furthermore, where experts identified potential solutions with significant drawbacks, solutions were removed.

The following process of selection and elimination was followed:

Step	Assessment	Action
1	Experts agreed that backups were the only solution which allowed for the recovery of data	Backups selected
2	None of the experts identified security awareness training as having an impact that did not require human interaction	Security awareness training eliminated
3	Application whitelisting was identified by experts as having the most operational/overhead, making it difficult to implement and maintain	Application whitelisting eliminated
4	Firewalls were not identified by experts as having a significant impact on overall coverage, and was the only capability with no votes in this category, limiting it's ability to reenforce other solutions	Firewalls eliminated
5	Email security suites were not identified by experts as having any impact on propagation, limiting it's ability to reenforce other solutions	Email security suites eliminated
6	Role based access controls were identified by experts as providing less coverage than patches and anti-virus, additionally role based access controls were identified by experts as being more difficult to implement and maintain	Role based access controls eliminated
7	Patches and anti-virus remain and were identified by experts as providing both significant coverage and capabilities to reduce propagation	Patches and anti-virus selected

Following this process resulted in the identification of backups, patches, and anti-virus as the strongest solution set which experts indicate aligns with the anti-ransomware strategy. The results for each analysis type leveraged are listed below:

Figure 15 – Subject Matter Expert Commentary Solution Sets Overview

Analysis / Solution	Quantitative	Subjective	Qualitative	Total
Backups	Yes	Yes	Yes	3
Patches	Yes	No	Yes	2
Anti-virus	Yes	Yes	Yes	3
Application Whitelisting	No	Yes	No	2

This table shows that regardless of the analytical methodology, backups and anti-virus were identified by experts as key to an anti-ransomware capability. Patches and application whitelisting compliment this set, with the key difference being a trade-off between effectiveness (application whitelisting) and ease of implementation and management (patches.) Review of the experts commentary also resulted in the determination that none of the eight potential solutions provide any significant level of protection against unknown threats. This indicates that any combination of capabilities will remain vulnerable to emergent ransomware, increasing the need for backups as an essential solution to respond when other capabilities fail.

Subject Matter Expert Commentary Solution Sets:

- ✔ Anti-virus, backups, and patches (quantitative, qualitative)
- ✔ Anti-virus, backups, and application whitelisting (subjective)

Survey Results

In order to offset inherent bias and to understand the requirements for deploying each ransomware solution, the Ellis Research Institute created a survey which asked respondents to rank the anti-ransomware solutions according to a variety of factors. This survey was largely focused on the costs, both budgetary and operational, related to each solution and included fifteen questions. These results were then reviewed to identify solutions which would be appropriate for organizations of varying sizes and internal capabilities.

Of the sixteen respondents, which included this paper's author, 50% (eight respondents) indicated that they have dealt directly with ransomware incidents in the past. Respondents identified themselves as having the following focuses:

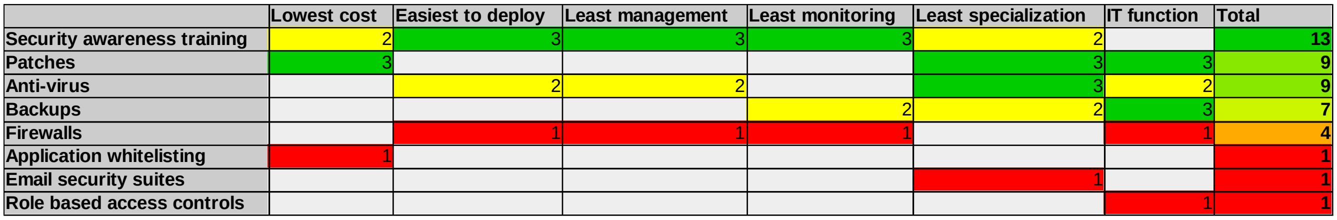
- 81.25% have conducted defensive operations (thirteen respondents)
- 62.5% have been involved in threat intelligence (ten respondents)

- 43.75% have an IT focus (seven respondents)
- 37.5% identified themselves as having an offensive security background (six respondents)

The respondents were split across those with management roles (seven respondents) and those with analyst or engineering roles (nine respondents) and had an average of 16.93 years of experience in their respective industries.

In order to frame the overall results in a useful manner for organizations with limited cyber security staff, budget, and expertise respondents were asked to rank capabilities according to their difficulty to deploy, manage, and monitor, the capability's requirement for specialized training, and the capability's total cost of ownership. These results were then organized based on the number of affirmative responses and a set of inverse votes were applied based on each solution's ranking.

Figure 16 – Survey results for costs and operational overhead



	Lowest cost	Easiest to deploy	Least management	Least monitoring	Least specialization	IT function	Total
Security awareness training	2	3	3	3	2		**13**
Patches	3				3	3	**9**
Anti-virus		2	2		3	2	**9**
Backups				2	2	3	**7**
Firewalls		1	1	1		1	**4**
Application whitelisting	1						**1**
Email security suites					1		**1**
Role based access controls						1	**1**

The respondents answers showed organizations with limited resources and constrained budgets should focus on security awareness training, patches, and anti-virus. These solutions were largely considered to have the fewest requirements for the organization looking to deploy them. Furthermore, each of these solutions have a function that goes beyond purely defending against ransomware, so they will provide additional protections in other scenarios. When skill sets and the size of the security team itself were considered as the primary limiters backups, anti-virus, and patches were identified as a good solution set as they can be largely managed by existing IT staff.

As part of the survey, respondents were also asked to rank the effectiveness of each solution. Each capability was scored based on its overall rank. This ranking resulted in the identification of backups, patching, and either security awareness training or email security solutions as the recommended defenses for ransomware.

Survey Solution Sets

- ✔ Anti-virus, patches, security awareness training (costs)
- ✔ Anti-virus, patches, backups (costs)
- ✔ Backups, patches, email security suites (rankings)
- ✔ Backups, patches, security awareness training (rankings)

Phase 3 – Solutions Review

Real World Data

Ransomware is a common occurrence and as such many examples exist which can be used as test cases for the solution sets identified in this paper. The Ellis Research Institute selected six well known ransomware variants for which in-depth behavioral analysis has been conducted by industry experts. These variants included both opportunistic and targeted samples spanning a four year period from 2013 through 2017. The ransomware variants chosen were: CryptoLocker (2013), SamSam (2016), Locky (2016), Petya (2016), NotPetya (2017), and WannaCry (2017.)[23]

Each ransomware variant has been analyzed by at least one external source who identified its specific modes of operation, characteristics, and capabilities. This information was collected and reviewed to determine which of the eight recommended capabilities would have prevented or mitigated the threat. These results were then compared against the solution sets created throughout the analysis phase to determine which combinations of solutions would prevent each variants. The Figure 17 aligns each anti-ransomware capability with the selected ransomware variants, indicating if mitigation would have occurred.

Figure 17 – Anti-ransomware capabilities by variant

	WannaCry	CryptoLocker	Locky	Petya	NotPetya	SamSam	Total
Patches	Yes: Patches existed prior to attack[24]	No: Delivered by other malware[25]	Yes: Patches existed prior to attack[26]	No: Does not leverage exploits[27]	Yes: Patches existed prior to attack[28]	Yes: Patches existed prior to attack[29]	4
Backups[1]	Yes	Yes	Yes	Yes	Yes	Yes	6
Security awareness training	No: Does not require user interaction[30]	Yes: Requires opening a malicious email attachment[31]	Yes: Requires opening a malicious email attachment[32]	Yes: Requires opening a malicious email attachment[33] Requires user authorize UAC bypass[34]	No: Delivered by compromised tax software and leveraged EternalBlue[35]	Yes: Leveraged weak passwords[36]	4
Email security suites	No: Not delivered by email[37]	Yes: Delivered by email attachment[38]	Yes: Delivered by email attachment[39]	Yes: Delivered by email attachment[40]	No: Delivered by compromised tax software and leveraged EternalBlu[41]	No: Not delivered by email[42]	3
Role Based Access Controls[2]	Partial: Prevents file-share and stolen credential based activities; however, also leverages exploitation[43]	Yes: Does not spread and only encrypts local/network accessible files[44]	Yes: Does not spread and only encrypts local/network accessible files[45]	No: Corrupts the MBR rather than discrete files[46]	Partial: Prevents file-share and stolen credential based activities; however, also leverages EternalBlue[47]	Partial: Prevents file-share and stolen credential based activities[48]; however, also leverages EternalBlue[49]	3.5
Anti-virus	Yes: Exploit signatures existed prior to deployment[50]	No: Delivered to already infected hosts[51]	Yes: Exploit/anti-ransomware signatures existed prior to deployment[52]	Yes: Exploit signatures existed prior to deployment[53]	Yes: Exploit and Mimikatz signatures existed prior to deployment[54]	Yes: Exploit signatures existed prior to deployment[55]	4
Application whitelisting[3]	Yes	Yes	Yes	Yes	No: Deployed by trusted software[56]	Yes	5
Firewall	Yes: Spread via exposed SMB ports[57]	No: Does not attempt to spread[58]	No: Does not attempt to spread[59]	No: Does not attempt to spread[60]	Yes: Spread via exposed SMB ports[61]	Yes: Spread via exposed RDP ports[62]	3

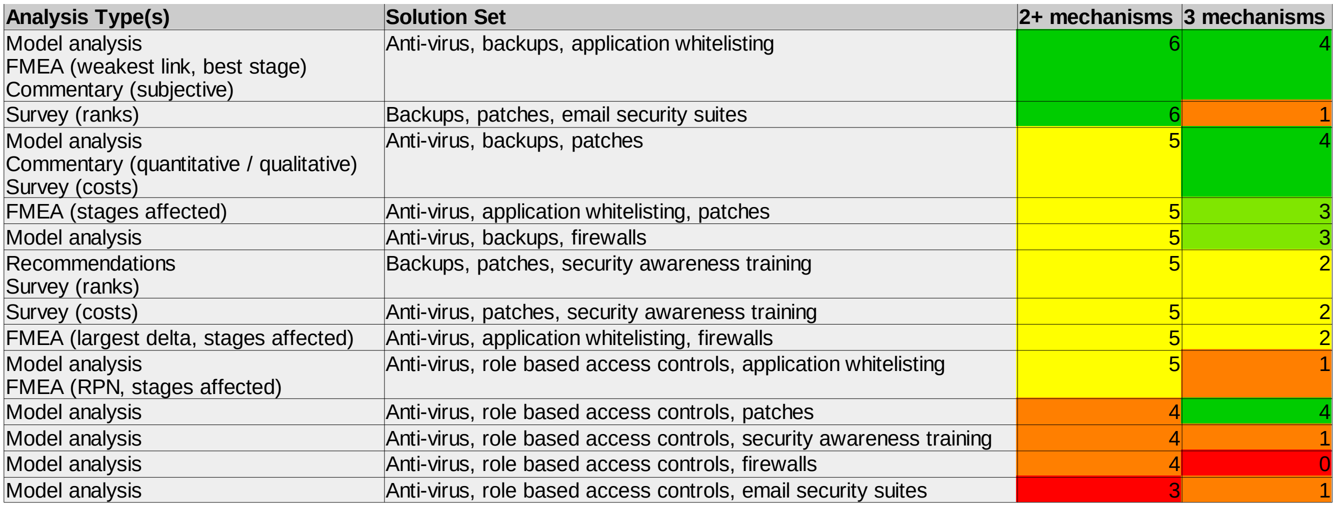
This table shows that, except for backups, no single capability is effective against all six variants of ransomware. While backups can be seen as a universal anti-ransomware capability, it is only effective after damage has been done, rather than preventing the occurrence of ransomware. These results clearly

[1] Backups apply across all forms of ransomware as long as they are sufficiently isolated
[2] Role based access controls may only be effective when paired with patches to mitigate exploitation
[3] Application whitelisting generally applies as it prevents the execution of unknown code

illustrate the need for a multifaceted strategy for defending against ransomware with capabilities which reenforce each other.

Each of the thirteen solution sets identified during the analysis phase were compared to this table to understand how many variants would be mitigated and by how many capabilities. These results were ranked first by how many variants were prevented by at least two capabilities, then by how many were prevented by all three capabilities. This ranking is based on a "weakest link" analysis, in that a solution set with only five of six variants being prevented by two solutions lacks depth of defenses across all potential threats. The table below lists the solution sets, which analysis techniques produced them, and how many ransomware variants would have been rendered ineffective by one, some, or all of the capabilities.

Figure 18 – Anti-Ransomware Solution Set Effectiveness



Analysis Type(s)	Solution Set	2+ mechanisms	3 mechanisms
Model analysis FMEA (weakest link, best stage) Commentary (subjective)	Anti-virus, backups, application whitelisting	6	4
Survey (ranks)	Backups, patches, email security suites	6	1
Model analysis Commentary (quantitative / qualitative) Survey (costs)	Anti-virus, backups, patches	5	4
FMEA (stages affected)	Anti-virus, application whitelisting, patches	5	3
Model analysis	Anti-virus, backups, firewalls	5	3
Recommendations Survey (ranks)	Backups, patches, security awareness training	5	2
Survey (costs)	Anti-virus, patches, security awareness training	5	2
FMEA (largest delta, stages affected)	Anti-virus, application whitelisting, firewalls	5	2
Model analysis FMEA (RPN, stages affected)	Anti-virus, role based access controls, application whitelisting	5	1
Model analysis	Anti-virus, role based access controls, patches	4	4
Model analysis	Anti-virus, role based access controls, security awareness training	4	1
Model analysis	Anti-virus, role based access controls, firewalls	4	0
Model analysis	Anti-virus, role based access controls, email security suites	3	1

Note: Role based access controls were only considered effective against SamSam, NotPetya, and WannaCry when combined with patching, which mitigated exploitation capabilities

The results of this comparison shows that anti-virus, backups, and application whitelisting are the most effective combination – providing at least two mechanisms for defeating each type of ransomware. The second most effective solution set, backups, patches, and email security suites, also prevented six out of six variants with at least two capabilities, but only one with all three. All other solutions had at least one ransomware variant which had only one control in place, often backups meant for recovery, leaving a weak spot which could be exploited.

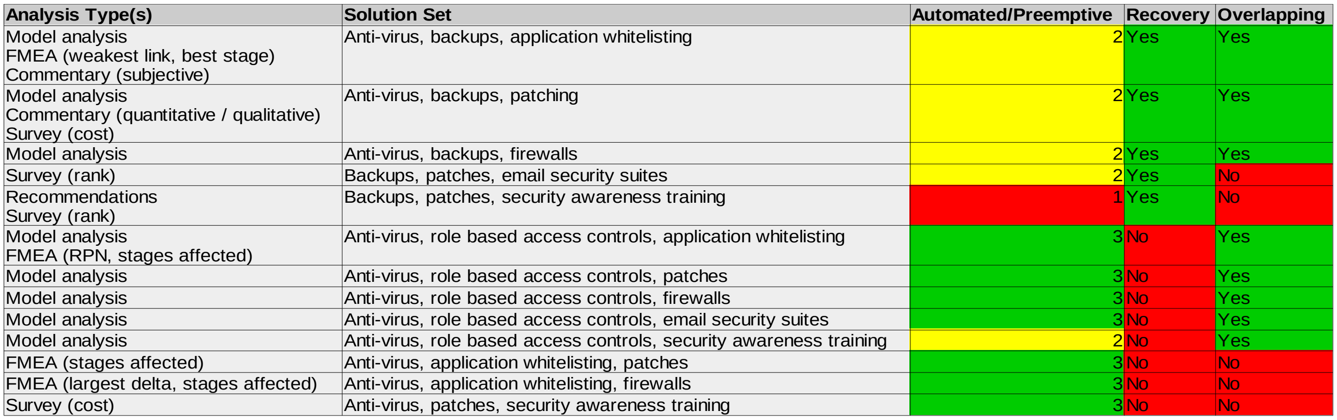
When the cost and overhead is a limiting factor, the third solution set did provide reliable coverage across five of the six variants. This solution set included backups, which would provide a fail-safe for the sixth variant (CryptoLocker), should it have been deployed by the organization.

The top four solutions were identified, at least in part, by either the subject matter expert commentary or the survey of cyber security experts. The only other solution identified by experts, tied for seventh place, was identified specifically as part of the cost effectiveness portion of the survey.

Strategic Review

Each solution set identified during the analysis phase was also compared against the anti-ransomware strategy laid out at the beginning of this paper. This review was designed to determine if a solution set provides automated or preemptive controls which overlap to provide resilience, while also providing the ability to recover from a successful ransomware outbreak. Automated and preemptive solutions included all capabilities except for security awareness training, which requires users to take action, and backups, which are only useful after the destruction of data. While multiple solutions were able to limit the impact of an outbreak, only backups provided the ability to recover in the event that ransomware is successful. Overlapping solutions were identified by the Cyber Modeling Framework analysis and specifically looked for combinations of solutions which reenforced each other. Below is a table which aligns each of the thirteen solution sets identified with these key strategic objectives.

Figure 19 – Solution set adherence to the anti-ransomware strategy



Analysis Type(s)	Solution Set	Automated/Preemptive	Recovery	Overlapping
Model analysis FMEA (weakest link, best stage) Commentary (subjective)	Anti-virus, backups, application whitelisting	2	Yes	Yes
Model analysis Commentary (quantitative / qualitative) Survey (cost)	Anti-virus, backups, patching	2	Yes	Yes
Model analysis	Anti-virus, backups, firewalls	2	Yes	Yes
Survey (rank)	Backups, patches, email security suites	2	Yes	No
Recommendations Survey (rank)	Backups, patches, security awareness training	1	Yes	No
Model analysis FMEA (RPN, stages affected)	Anti-virus, role based access controls, application whitelisting	3	No	Yes
Model analysis	Anti-virus, role based access controls, patches	3	No	Yes
Model analysis	Anti-virus, role based access controls, firewalls	3	No	Yes
Model analysis	Anti-virus, role based access controls, email security suites	3	No	Yes
Model analysis	Anti-virus, role based access controls, security awareness training	2	No	Yes
FMEA (stages affected)	Anti-virus, application whitelisting, patches	3	No	No
FMEA (largest delta, stages affected)	Anti-virus, application whitelisting, firewalls	3	No	No
Survey (cost)	Anti-virus, patches, security awareness training	3	No	No

Of the thirteen solution sets, only three met all of the criteria laid out in the anti-ransomware strategy. These solution sets all included anti-virus and backups, with the choice of either application whitelisting, patching, or firewalls. It is important to note that the recovery objective could only be met by including backups in the solution set, which is not an automated or preemptive solution. Due to this, solution sets in which all three capabilities were automated or preemptive could not fulfill this requirement and therefore ranked lower in this assessment.

The choice between patches and application whitelisting largely comes down to a question of ease of deployment versus effectiveness, respectively. The solution set containing firewalls was only identified by the model analysis, indicating that while it may represent a strategically valid solution, it is not optimized for any specific use case.

Conclusions

The Ellis Research Institute began this ransomware analysis with two goals – to prioritize solutions which defend against ransomware and to identify a methodology which could be applied to cyber security threats in general. This process began by defining the problem of ransomware and developing a high level strategy for mitigating the threat it poses. Following this definition phase, multiple analysis techniques were used to review eight different capabilities which are commonly referenced in anti-ransomware guidance. The analysis results were compared against real-world ransomware examples and the anti-ransomware strategy to determine which would be effective in practice. Finally, the analysis techniques, and their combinations, which produced each solution set were reviewed to understand which were most and least effective at predicting the recommended solutions.

Recommended Ransomware Solutions

After conducting five types of analysis across the eight different capabilities, the Ellis Research Institute produced thirteen different solution sets. Each solution set, composed of three capabilities, was tested using two different review techniques and the top three solutions from each review were identified as the potential "best" solution sets. The real-world data review produced a ranked set of results, whereas the qualitative strategic review identified three solutions which met all of the required criteria. These solution sets were:

Real-World Data Review

1. Anti-virus, backups, application whitelisting
2. Backups, patches, email security suites
3. Anti-virus, backups, patches

Strategic Review

- Anti-virus, backups, application whitelisting
- Anti-virus, backups, firewalls
- Anti-virus, backups, patches

Two solution sets were present in both lists, indicating that they represent the ideal defenses against ransomware. These solution sets both included anti-virus and backups and offered a choice between application whitelisting and patches. Both solution sets were identified as front runners by three of the five analysis techniques, with the Cyber Modeling Framework analysis and commentary provided by subject matter experts agreeing on both. Patches were identified by the survey conducted, which focused primarily on the costs and overhead associated with each capability. Conversely, application whitelisting was identified by the Failure Mode and Effects Analysis, which focused primarily on the overall effectiveness of each capability. Both solution sets represent strong options providing the ability to recover from a ransomware outbreak, redundancy in defenses, and capabilities which are proactive or automatic in their response to a ransomware event as it occurs. The choice between these two solution sets falls largely on an organization's ability to deploy and support application whitelisting. For organizations that can manage application whitelisting, the combination of solutions represents the most effective defense against ransomware. For organizations that need minimize overhead, the combination of solutions including patches trades a degree of effectiveness for a more realistic suite of capabilities.

Recommended Solution Sets:

Most Effective

- Anti-virus
- Backups
- Application whitelisting

Cost Effective

- Anti-virus
- Backups
- Patching

Analysis Methodology Review

Throughout this paper the Ellis Research Institute leveraged five different analysis techniques and two different testing techniques to review potential solutions to the threat of ransomware. These techniques ranged in the level of subjective, qualitative, and quantitative analysis conducted and produced varied results. Each technique approached the problem from a different view point and their wider applications have different contexts. While it was possible to make determinations using each, it is important to note the strengths, weaknesses, and effectiveness of each methodology.

In terms of effectiveness and judged based on which solution sets ranked highest in both the real-world data and strategic reviews, the subject matter expert commentary was the best predictor of effective solution sets. Both of the recommended solution sets were identified by these experts and furthermore were the only solution sets which the experts agreed upon. While these results may be biased by the prevalence of ransomware and the quality of the experts, this is a strong predictor that any threat analysis should include input from multiple cyber security experts.

While the survey results were not a strong predictor of the best solution sets, it did provide useful data for understanding the realistic challenges around implementing each capability. In many cases, the most effective solution sets to real-world cyber security problems will include capabilities which are prohibitively expensive, difficult to deploy, or require significant overhead to maintain. It is important to ensure that any solutions analysis includes a component that prioritizes realistic solutions to ensure that the results are not merely academic.

The analysis of the model produced by the Cyber Modeling Framework was also able to predict both of the recommended solutions; however, it also identified five other solution sets including those ranked worst by both testing techniques. While this analysis technique was useful for defining the problem and identifying solutions which provide a depth of defenses, it’s wide range of outputs makes it impractical to use as a stand-alone analysis methodology. The value provided by this analysis technique could increase if additional data was included in the model, such as connecting it directly with the Failure Mode and Effects Analysis; however, this combination only produced one of the top two solutions identified in this paper and also identified less optimal solutions.

Based purely on the results of this paper, the combination of the model analysis, subject matter expert commentary, and a Failure Mode and Effects analysis focused on optimizing for the weakest link produced the most effective set of capabilities. When viewing the capabilities survey as another form of expert review, this combination of analysis techniques can also be used to identify a most cost effective solution. While certain analysis techniques were less effective overall, it is important to note that each methodology required a different mindset and for unknown or emergent threats, may be useful to help analysts, strategists, and managers understand a problem better. Additional notes on each analysis technique can be found in Appendix F.

Appendix A – Capability Definitions

Anti-virus is any end-point software designed to detect and prevent malicious activity by means of signatures or behavioral patterns.

Application whitelisting is any end-point software designed to detect and prevent malicious activity by maintaining a list of authorized software and denying execution to any unapproved software.

Backups are any solution designed to retain copies of data, configurations, transactional records, or other critical data which can be used for restoration in the event that corruption occurs.

Email security suites are any solution designed to interdict emails by detecting malicious attachments or links.

Firewalls are any solution designed to limit network activity by means of blocking traffic to specific hosts or ports.

Patches are any updates to software or operating systems which are designed to resolve vulnerabilities.

Role based access controls (RBAC) are any solution designed to limit access to files or directories based on user-level permissions. Access may be entirely denied or limited to read-only capabilities.

Security awareness training is any activity directed by an organization for informing employees about best practices, proactive behaviors, or emergent threats designed to prevent bad actors from compromising devices or accounts.

Appendix B – Subject Matter Experts

Cyber Security and Information Technology Experts

Michael J. Rose
Principal Security Architect, Rose Security

Charlie Briggs
VP Information Security and Technical Lead

Mark St. John
Founder and Chief Operations Officer, AlphaWave

Eric van Leeuwen
Linux Systems Administrator

Andrew C. Ellis GSEC, GCIA
Director of Global Threat Management, GameStop
Founder and Director, Ellis Research Institute

Continuous Improvement Experts

John Ellis PMP
Sr. Manager Continuous Improvement Strategic Project Portfolio, Human Resources and Legal, NEC Corporation of America

Appendix C – Subject Matter Expert Commentary

Experts listed below have been made anonymous and assigned an “expert ID” which is used for references. Responses are included as they were provided by the experts, with only formatting changes made.

Commentary Request

I am currently writing a paper on selecting security capabilities to deal with the threat of ransomware. As part of this process, I am seeking out expert commentary on a set of solutions collected from a variety of industry recommendations. I don't have any specific format or desired deliverable for your response, only your collection of thoughts on any/all of these optional capabilities. Once I have responses from each expert, I will be consolidating these along with my own thoughts to enhance the overall analysis. Please note that your responses will be presented, in an anonymized fashion, in the final version of this publication. If you would like your name to be included in the references appendix, please let me know. If you are uncomfortable with my including your thoughts in this analysis, please disregard this request.

The list of solutions which can be used to protect against or mitigate the threat of ransomware are:

- Patching
- Anti-virus
- Backups
- Role-based access controls (RBAC)
- Email security solutions
- Security awareness training
- Application whitelisting
- Firewalls

Subject Matter Expert #1

The first thing to note when dealing with ransomware, as with any cyber security threat, is that no one solution, technology, or tool will be able to protect against it on its own. Defense in depth is key, with a multi-layered strategy being the best way to keep data safe from ransomware. With ransomware I would consider there to be three stages of an effective strategy; stopping the initial infection, limiting lateral infections, mitigating encryption of infected systems. Of those capabilities listed below, the first and the last stages are addressed, but minimal attention is paid to the middle stage when, arguably, this is the most important. In cases of successful ransomware infection, the ability to block lateral or follow-on infections can stop an annoying but resolvable problem from turning into something that can impact all business operations and lead to a business shuttering. With that being said;

Patching

Patching does not directly protect against ransomware, but rather reduces the risk of being vulnerable to an exploit that allows for a ransomware infection to take hold, or that allows it to replicate and spread throughout an environment. I would consider patching to be an IT function primarily, with the security impact being a valuable side effect. That's obviously ignoring patches released to specifically address high priority security issues that can be exploited despite other security protections that might be in place.

Anti-virus

Considering AV to be endpoint software designed to detect and block malicious code from running on a target system, it definitely is a strong component of any anti-ransomware strategy. As end user systems are a significant infection vector for ransomware, anything that can directly protect them is advantageous. Additionally, AV tends to be fairly low cost, low effort (install, configure update schedule, monitor for alerts) with a good return on investment. AV does require signatures or heuristic characteristics to be written for given threats, so there is likely to be lead time between when a threat is identified and when the AV is able to protect against it. This can give a false sense of security especially against targeted and motivated attacks.

Backups

Having backups of data is an essential step to mitigate the effects of a successful ransomware infection. If data can be recovered from backup without any significant loss, then there is no need to pay any ransom to recover encrypted data. Obviously in such a case the backup does not protect against reinfection, so rather than just recovering immediately from backup, it is a better strategy to identify the infection vector, address that, then recover from backup. For a backup to be effective in mitigating a ransomware infection it must have four characteristics; completeness (contain all data required for business continuation), recency (contains data new enough to be of value), be verified (recovery of data has previously been confirmed to be successful), and be disconnected (not directly connected to infected systems such that the ransomware encrypts the backup also).

RBAC

Depending on the definition of RBAC used, limiting a user's access can be an excellent way to address the middle stage (limiting lateral infections) of a ransomware infection. A classic example of a devastating ransomware attack is a user system getting compromised then the encryption spreading to data on a network share mounted on the infected system. If the user only requires read only access and it is enforced through RBAC, then they will have no ability to modify the data on the network share, stopping the lateral infection immediately. This can also be addressed by such technologies as Zero Trust networking (a stretch of the RBAC term, but a valid one I feel in this case) which, if appropriately configured, can stop the migration of an infection from one system to another, simply by blocking such network traffic regardless of the intent. This can become very complicated to manage, and has the potential to impact productivity if enabled too zealously, so should likely be planned out prior to implementation, and operated in a 'report don't block' mode initially if such functionality is available.

Email Security Solutions

Email is one of the two primary infection vectors for ransomware, and as such anything that can help protect users from email-borne threats is a positive. Email security solutions tend to fall into one of two types, with some significant overlap in functionality; anti-spam and anti-malware. Spam email originally referred to unwanted but not inherently malicious email, such as pump and dump stock mails. However, overtime benign but spammy messages have declined, and most spam mail can be considered to be malicious rather than just annoying. For an email security solution to be effective against ransomware it needs to be able to address the two ways in which an email message can be malicious, either a direct attachment (say, weaponized PDF) or links to externally hosted malicious code. The former is fairly well addressed by email server anti-virus type solutions, but the latter can be fairly hard to address without significant risk of false positives. This is likely better addressed by user education as noted below.

Security Awareness Training

Users are the weakest link in any security chain, so anything that can be done to educate them on being more secure is a net positive. However, the training has to be written in such a way to educate users, rather than simply address compliance requirements as is common with a lot of corporate training programs, especially in large corporations.

Application Whitelisting

Ignoring the small percentage of malware specifically designed to get around whitelisting, application whitelisting can be the most effective defense against ransomware. Application whitelisting works by only allowing trusted and approved code to run, and any even slight deviation from that will simply be denied execution.1 This, however, turns a security problem into a useability problem, depending on the homogeneity of systems in an environment, and the expected functions of employees. For example, white listing is a perfect solution for the workstations bank tellers use to process customer deposits and withdraws. There is a standard gold image, no ad-hoc modifications should be made to that, and any updates or changes have to go through a long approval process prior to deployment. However, for a software engineer this would likely get productivity impacting very quickly as they try, and fail, to legitimately run random otherwise unapproved code to perform their day to day function.

Firewalls

If we consider firewalls to mean traditional firewalls that simply separate "us" from "them", segregating internal systems from the outside internet as a whole, then their impact in protecting against ransomware is minimal. Given that the majority of ransomware infections are caused by user activities such as visiting compromised websites or clicking links in malicious emails, this activity will not be affected by inside/outside firewall configuration. For firewalls to be helpful in a ransomware strategy, they must be configured to control east/west traffic that can stop lateral infections. While this is simple in theory, the practicalities of such configuration in anything but the most minimal environment can make it impossible to mitigate such lateral movement while still being manageable. Obviously this does not affect the value a well configured traditional firewall can have in protecting against other cyber security threats. Even the most ardent proponent of 'post compromise security tooling' will still see significant value in using firewalls.

Subject Matter Expert #2

Patching

The timely application of security patches alone is not sufficient to prevent ransomware. However, it is still a recommended action to avoid other known threats, and may help to limit potential exposure to ransomware spread through worm-like attacks. To expand on this, ransomware may be spread due to the presence of a vulnerability in the operating system or third party software, however fully patched systems can still be subjected to ransomware attacks.

Anti-virus

Anti-virus, anti-malware and EDR tools offer good defenses against known ransomware signatures and behaviour. Ensuring these products and their respective definitions are kept up to date is a key factor in reducing the risk of exposure here. In addition, exclusion lists need to be carefully monitored - if ransomware is downloaded to a folder within the exclusion list, it is possible that the actions will not be flagged.

Backups

Although this is not a prevention measure, it is incredibly important to ensure regular backups are made of all sensitive data. The backup data should be stored off-site in a location unreachable by the primary machine, otherwise the backup data could potentially become encrypted by the ransomware following an infection. Although data may be recoverable by paying the ransom, it is noted that there have been cases where files locked by ransomware cannot be decrypted due to the group behind the attack not providing the key. Refer to the case at Kansas Heart Hospital for further information. In short, to avoid financial losses as well as unrecoverable data, make sure you have everything backed up!

Role-based access controls (RBAC)

Correct application of access controls is a good way to avoid, or at least limit, the effects of ransomware. Controlled folder access (CFA) is a protection measure available in Windows 10 which, when enabled, will monitor, detect and block any changes made to the specified folders and their contents. Similar to AV, exclusions can be made which can compromise the effectiveness of this. For example, if a user was to regularly use PowerShell in their job they may need to allow powershell.exe to modify certain files/folders, and if a piece of ransomware used powershell.exe as part of the attack, this would not be detected or blocked.

In addition to CFA, traditional RBAC can be used to reduce the likelihood of a ransomware attack succeeding by following the principle of least privilege. Sensitive files should be edited by elevated users and remain unavailable for modification to regular users. Although this can decrease usability, it means that if a piece of ransomware was executed by a regular user, it would run under that user's context and, as the regular user will lack the permissions required to encrypt certain sensitive files, the ransomware would be unable to encrypt the protected files.

Email security solutions

Email is the most common delivery mechanism for malware/ransomware, so implementing security solutions to scan email content, strip attachments, or note that the sender is an external party can be a good defensive measure. With modern email clients, including web-based ones like Gmail, payload delivery by email has become more difficult to achieve due to a number of these protection measures being enabled by default. However, there are various methods which can be used to ensure a successful payload delivery, such as providing a link to a web server hosting the payload, storing the executable inside a password-protected ZIP file (which cannot be scanned) or, in a corporate setting, phishing a user and using that account to send the payload internally so it is trusted.

Security awareness training

Training, and regular reminders, can help to limit the likelihood of a successful ransomware attack in a corporate setting. However, even the most cautious of users can still fall victim to well-coordinated and sophisticated attacks. The training currently offered essentially boils down to "do not click links", which is somewhat unhelpful given how the internet works, so a lot of effort should be invested into proper training to allow for understanding of security best practices. Training in itself will not be enough to defend against ransomware, however. For example, if a legitimate website were to be compromised and used to spread malware, an end user may correctly follow all guidance regarding checking the hostname, presence of HTTPS, and even things like domain registration records, but would still become a victim if they proceeded with the download.

Application whitelisting

Implementing a whitelist of allowed applications is a good defense against malware in general, however a number of bypasses to popular whitelisting solutions (e.g. AppLocker) are known and regularly being researched, therefore it cannot solely be relied on.

Firewalls

In some settings, this may be a sufficient defense by allowing inbound and outbound connections to only trusted hosts. However, in a typical corporate network or a home network, this would not be a feasible approach to prevent ransomware, as delivery via the web could come from almost any hostname or IP. Although it may be possible to implement a blacklist of known malicious hosts, payloads could be hosted by cloud infrastructure services, like AWS or Azure, or on legitimate sites which have been compromised, meaning blocking access to these would be difficult. Reducing/limiting outbound connectivity will also have no effect on the successfulness of the ransomware attack as, opposed to C2 channels, ransomware will typically not need to communicate back to the origin once deployed.

In addition to the list provided above, I've got another point to add:

Virtual machines/containerisation

In my line of work, a lot of what I do is inside virtual machines. To avoid any data loss, regular snapshots are taken - this allows me to easily revert back to a safe state. In addition, due to the guest/host segregation, if files were to become encrypted in the VM, providing shared folders are not enabled, it would have no effect on the underlying host unless the group behind the ransomware attack had implemented a sandbox escape exploit, which is unlikely to be burned when it could be sold to exploit brokers, used in competitions, or rewarded through bug bounty programmes.

Subject Matter Expert #3

As a sysadmin I'd prioritize Backups over all the other solutions. Each mitigation has it's place and differently counters any of the various ways ransomware gets into an environment. Patching, RBAC, education, and filtering (probably in that order) are the best counters for spray and pray or phishing varieties of ransomware ingress. In the case of advanced teams targeting an organization and implementing a more custom/manual ransomware infiltration the fronts of firewall, segmentation, and application whitelisting would prove to be more effective in _slowing_ the infiltration.

Subject Matter Expert #4

Patching

Pros: Minimizes footprint for attacks to use automated and canned exploits. Forces them to find harder targets or exhaust automation and move to new targets.

Cons: A constant administrative battle for IT and DevOps. Constant release cycles requires constant deployment cycles.

Anti-virus

Pros: Gets rid of low hanging fruit binaries, published rootkits and other repackaged and unmodified/non custom attacker tools.

Cons: Hash and other pattern matching is often behind the times on releasing current “in the wild”. Requires full time administration of inventory upkeep to ensure agent coverage.

Backups

Pros: Enables rebuild the environment after mitigation quickly. Inspires confidence in responders that their efforts can be to a restored, clean environment. Allows responders to take quick, efficient, sometimes dramatic actions to remediate that some without backups don’t have the luxury of doing.

Cons: Expensive at scale

Role-based access controls (RBAC)

Pros: Limit scale of compromised credentials. Limit remediation scope of compromised accounts.

Cons: Administration in larger environments can be a burden.

Email security solutions

Pros: Help provide extra layer of protection for end users. Provide extra intelligence value to your internal security teams.

Cons: Many still allow a user override, links can be copy/pasted. An argument could be made they reinforce bad habits.

Security awareness training

Pros: Keeps users up to date information, habits to make and new technology to leverage

Cons: If “user shaming” is part of the training, leads to apathetic behavior

Application whitelisting

Pros: Provides strict guidance on what is allowed in an environment

Cons: Crafty users will create ShadowIT. Creates a barrier between IT and users.

Firewalls

Pros: Can help limit internal, lateral movement. External firewall slowly phasing out in an RBAC/Zero Trust world

Cons: Rules management overhead is cumbersome.

Subject Matter Expert #5

Patches

Pros: Patching systems has security and IT benefits beyond exclusively ransomware. Patches are likely already be part of existing security of IT programs. Patches do not require monitoring to be effective.

Cons: Patches may require a team to verify their deployment does not cause issues and is applied ubiquitously. Patches only prevent a sub-set of known vulnerabilities.

Backups

Pros: Backing up data in case of destruction has benefits beyond exclusively remediating ransomware. Backups are likely to already be part of existing disaster recovery programs. Backups have a relatively low resource investment as they do not require 24/7 monitoring. Backups are essential to defending against ransomware, as they are the only method of remediating destroyed data.

Cons: Backups require regular verification that they can be used for complete recovery. Backups can be difficult to implement ubiquitously. Backups do not prevent any malicious action, only allowing for remediation.

Security Awareness

Pros: Security awareness training has benefits beyond exclusively preventing ransomware. Security training is likely to already be part of existing security programs.

Cons: Security training does not make end users security experts. Security training does little to stop ransomware outbreaks after they have begun.

Email Security

Pros: Email security has benefits beyond exclusively preventing ransomware. Email security platforms can be configured in automatic enforcement modes requiring minimal oversight. Implementation may allow for detecting of known and unknown threats.

Cons: Many threats do not source from emails and are therefor unaffected by any email security solutions. Email security solutions make require regular upkeep to ensure that legitimate email is not blocked. Only prevents the initial infection.

Role Based Access Controls

Pros: Role based access controls have benefits beyond exclusively limiting ransomware. Role based access controls make access to protected data by bad actors more difficult. Once configured, role based access controls will automatically disallow access and modifications to data.

Cons: Effective role base access controls may be difficult and time consuming to implement and maintain. Due to the interconnected nature of business, role base access controls may still allow for connectivity to protected resources through multiple “hops.”

Anti-virus

Pros: Anti-virus has benefits beyond exclusively protecting against ransomware. Anti-virus solutions can be configured to automatically block threats, preventing both initial infections and the spread of ransomware. Anti-virus solutions provide security logging which can be used as part of a monitoring or forensics program.

Cons: Anti-virus only protects against known and detectable threats.

Application Whitelisting

Pros: Application whitelists have benefits beyond exclusively protecting against ransomware. Application whitelists are more effective at preventing unknown threats. Application whitelisting solutions can be configure to automatically deny unauthorized execution. Application whitelisting solutions provide security logging which can be used as part of a monitoring or forensics program.

Cons: Application whitelisting may be difficult and time consuming to implement and maintain. Platforms such as end user devices may be difficult to enforce effective application whitelisting on.

Firewalls

Pros: Firewalls have benefits beyond exclusively protecting against ransomare. Firewalls are likely already part of network architectures. Once configured, firewalls will automatically block disallowed traffic.

Cons: Firewalls only prevent connectivity and once malware is present on a system it has all the access a legitimate user would. Due to the interconnected nature of networks and businesses, firewalls may still allow for connectivity to protected resources through multiple “hops.”

Appendix D – FMEA Scales

Below is a listing of the meaning behind scores for each component of the Failure Mode and Effects Analysis conducted on ransomware solutions.

Severity – measures the impact from each stage of a ransomware attack

Severity	
1	Recoverable negligible impact
2	Recoverable small scale impact
3	Recoverable medium scale impact
4	Recoverable large scale impact
5	Recoverable massive impact
6	Non-recoverable negligible impact
7	Non-recoverable small scale impact
8	Non-recoverable medium scale impact
9	Non-recoverable large scale impact
10	Non-recoverable massive impact

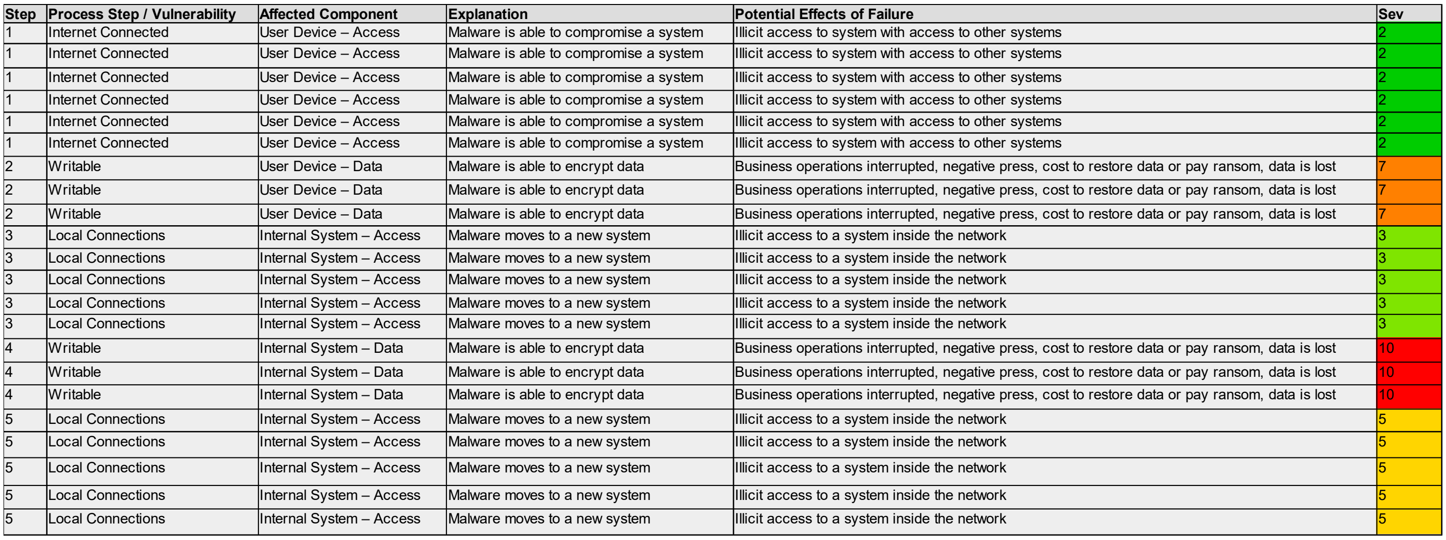
Occurrence – measures the likelihood of each stage of a ransomware attack

Occurrence	
1	Rare and massive difficulty for attacker
2	Rare and significant difficulty for attacker
3	Rare and moderate difficulty for attacker
4	Rare and minor difficulty for attacker
5	Rare and trivial difficulty for attacker
6	Frequent and massive difficulty for attacker
7	Frequent and significant difficulty for attacker
8	Frequent and moderate difficulty for attacker
9	Frequent and minor difficulty for attacker
10	Frequent and trivial difficulty for attacker

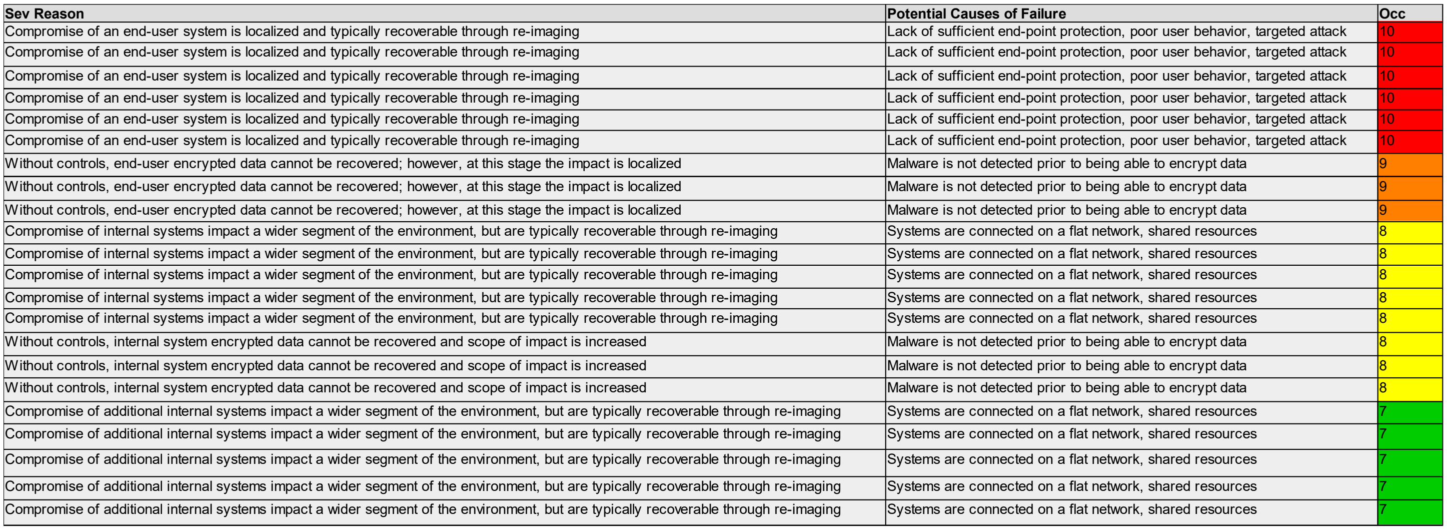
Detection – measures the potential to identify each stage of a ransomware attack

Detection	
1	High probability to detect prior to impact
2	Moderate probability to detect prior to impact
3	Low probability to detect prior to impact
4	High probability to detect during impact
5	Moderate probability to detect during impact
6	Low probability to detect during impact
7	High probability to detect after impact
8	Moderate probability to detect after impact
9	Low probability to detect after impact
10	No detection after impact

Appendix E – Full FMEA Table



Step	Process Step / Vulnerability	Affected Component	Explanation	Potential Effects of Failure	Sev
1	Internet Connected	User Device – Access	Malware is able to compromise a system	Illicit access to system with access to other systems	2
1	Internet Connected	User Device – Access	Malware is able to compromise a system	Illicit access to system with access to other systems	2
1	Internet Connected	User Device – Access	Malware is able to compromise a system	Illicit access to system with access to other systems	2
1	Internet Connected	User Device – Access	Malware is able to compromise a system	Illicit access to system with access to other systems	2
1	Internet Connected	User Device – Access	Malware is able to compromise a system	Illicit access to system with access to other systems	2
1	Internet Connected	User Device – Access	Malware is able to compromise a system	Illicit access to system with access to other systems	2
2	Writable	User Device – Data	Malware is able to encrypt data	Business operations interrupted, negative press, cost to restore data or pay ransom, data is lost	7
2	Writable	User Device – Data	Malware is able to encrypt data	Business operations interrupted, negative press, cost to restore data or pay ransom, data is lost	7
2	Writable	User Device – Data	Malware is able to encrypt data	Business operations interrupted, negative press, cost to restore data or pay ransom, data is lost	7
3	Local Connections	Internal System – Access	Malware moves to a new system	Illicit access to a system inside the network	3
3	Local Connections	Internal System – Access	Malware moves to a new system	Illicit access to a system inside the network	3
3	Local Connections	Internal System – Access	Malware moves to a new system	Illicit access to a system inside the network	3
3	Local Connections	Internal System – Access	Malware moves to a new system	Illicit access to a system inside the network	3
3	Local Connections	Internal System – Access	Malware moves to a new system	Illicit access to a system inside the network	3
4	Writable	Internal System – Data	Malware is able to encrypt data	Business operations interrupted, negative press, cost to restore data or pay ransom, data is lost	10
4	Writable	Internal System – Data	Malware is able to encrypt data	Business operations interrupted, negative press, cost to restore data or pay ransom, data is lost	10
4	Writable	Internal System – Data	Malware is able to encrypt data	Business operations interrupted, negative press, cost to restore data or pay ransom, data is lost	10
5	Local Connections	Internal System – Access	Malware moves to a new system	Illicit access to a system inside the network	5
5	Local Connections	Internal System – Access	Malware moves to a new system	Illicit access to a system inside the network	5
5	Local Connections	Internal System – Access	Malware moves to a new system	Illicit access to a system inside the network	5
5	Local Connections	Internal System – Access	Malware moves to a new system	Illicit access to a system inside the network	5
5	Local Connections	Internal System – Access	Malware moves to a new system	Illicit access to a system inside the network	5



Sev Reason	Potential Causes of Failure	Occ
Compromise of an end-user system is localized and typically recoverable through re-imaging	Lack of sufficient end-point protection, poor user behavior, targeted attack	10
Compromise of an end-user system is localized and typically recoverable through re-imaging	Lack of sufficient end-point protection, poor user behavior, targeted attack	10
Compromise of an end-user system is localized and typically recoverable through re-imaging	Lack of sufficient end-point protection, poor user behavior, targeted attack	10
Compromise of an end-user system is localized and typically recoverable through re-imaging	Lack of sufficient end-point protection, poor user behavior, targeted attack	10
Compromise of an end-user system is localized and typically recoverable through re-imaging	Lack of sufficient end-point protection, poor user behavior, targeted attack	10
Compromise of an end-user system is localized and typically recoverable through re-imaging	Lack of sufficient end-point protection, poor user behavior, targeted attack	10
Without controls, end-user encrypted data cannot be recovered; however, at this stage the impact is localized	Malware is not detected prior to being able to encrypt data	9
Without controls, end-user encrypted data cannot be recovered; however, at this stage the impact is localized	Malware is not detected prior to being able to encrypt data	9
Without controls, end-user encrypted data cannot be recovered; however, at this stage the impact is localized	Malware is not detected prior to being able to encrypt data	9
Compromise of internal systems impact a wider segment of the environment, but are typically recoverable through re-imaging	Systems are connected on a flat network, shared resources	8
Compromise of internal systems impact a wider segment of the environment, but are typically recoverable through re-imaging	Systems are connected on a flat network, shared resources	8
Compromise of internal systems impact a wider segment of the environment, but are typically recoverable through re-imaging	Systems are connected on a flat network, shared resources	8
Compromise of internal systems impact a wider segment of the environment, but are typically recoverable through re-imaging	Systems are connected on a flat network, shared resources	8
Compromise of internal systems impact a wider segment of the environment, but are typically recoverable through re-imaging	Systems are connected on a flat network, shared resources	8
Without controls, internal system encrypted data cannot be recovered and scope of impact is increased	Malware is not detected prior to being able to encrypt data	8
Without controls, internal system encrypted data cannot be recovered and scope of impact is increased	Malware is not detected prior to being able to encrypt data	8
Without controls, internal system encrypted data cannot be recovered and scope of impact is increased	Malware is not detected prior to being able to encrypt data	8
Compromise of additional internal systems impact a wider segment of the environment, but are typically recoverable through re-imaging	Systems are connected on a flat network, shared resources	7
Compromise of additional internal systems impact a wider segment of the environment, but are typically recoverable through re-imaging	Systems are connected on a flat network, shared resources	7
Compromise of additional internal systems impact a wider segment of the environment, but are typically recoverable through re-imaging	Systems are connected on a flat network, shared resources	7
Compromise of additional internal systems impact a wider segment of the environment, but are typically recoverable through re-imaging	Systems are connected on a flat network, shared resources	7
Compromise of additional internal systems impact a wider segment of the environment, but are typically recoverable through re-imaging	Systems are connected on a flat network, shared resources	7

Occ Reason	Current Process Controls	Det
End user devices are frequently targeted and are subject to a wide variety of tactics	None	10
End user devices are frequently targeted and are subject to a wide variety of tactics	None	10
End user devices are frequently targeted and are subject to a wide variety of tactics	None	10
End user devices are frequently targeted and are subject to a wide variety of tactics	None	10
End user devices are frequently targeted and are subject to a wide variety of tactics	None	10
End user devices are frequently targeted and are subject to a wide variety of tactics	None	10
End user devices, once compromised, can be trivially encrypted	Detection only occurs after files are rendered unusable	7
End user devices, once compromised, can be trivially encrypted	Detection only occurs after files are rendered unusable	7
End user devices, once compromised, can be trivially encrypted	Detection only occurs after files are rendered unusable	7
Internal systems, once compromised, can be used to pivot laterally assuming appropriate access is obtained by bad actor	None	10
Internal systems, once compromised, can be used to pivot laterally assuming appropriate access is obtained by bad actor	None	10
Internal systems, once compromised, can be used to pivot laterally assuming appropriate access is obtained by bad actor	None	10
Internal systems, once compromised, can be used to pivot laterally assuming appropriate access is obtained by bad actor	None	10
Internal systems, once compromised, can be used to pivot laterally assuming appropriate access is obtained by bad actor	None	10
Internal systems, when accessible and compromised, can be trivially encrypted	Detection only occurs after files are rendered unusable	7
Internal systems, when accessible and compromised, can be trivially encrypted	Detection only occurs after files are rendered unusable	7
Internal systems, when accessible and compromised, can be trivially encrypted	Detection only occurs after files are rendered unusable	7
Additional internal systems, when accessible and compromised, can be used to pivot laterally assuming appropriate access is obtained by bad actor	None	10
Additional internal systems, when accessible and compromised, can be used to pivot laterally assuming appropriate access is obtained by bad actor	None	10
Additional internal systems, when accessible and compromised, can be used to pivot laterally assuming appropriate access is obtained by bad actor	None	10
Additional internal systems, when accessible and compromised, can be used to pivot laterally assuming appropriate access is obtained by bad actor	None	10
Additional internal systems, when accessible and compromised, can be used to pivot laterally assuming appropriate access is obtained by bad actor	None	10

Det Reason	RPN	Recommended Actions	Effects of Change	Sev	Sev Reason
Undetected without controls	200	Application Whitelisting	Decreases likelihood of successful infection; Increases potential to detect failed infections	2	Does not decrease severity
Undetected without controls	200	Anti-virus	Decreases likelihood of successful infection; Increases potential to detect successful infections early	2	Does not decrease severity
Undetected without controls	200	Email security suites	Decreases likelihood of successful infection using email-based entry vectors;	2	Does not decrease severity
Undetected without controls	200	Firewalls	Decreases likelihood of infection through opened ports	2	Does not decrease severity
Undetected without controls	200	Security awareness training	Decreases likelihood of infection through email and browsers;	2	Does not decrease severity
Undetected without controls	200	Patches	Decreases likelihood of infection by reducing vulnerabilities	2	Does not decrease severity
Detected due to impact	441	Backups	Reduces severity of impact by allowing for recovery	2	Does not reduce scale, but allows for recovery
Detected due to impact	441	Anti-virus	Increases the likelihood of detecting malware and reduces potential for compromise	6	Reduces scale of impact by halting encryption early in the process
Detected due to impact	441	Role based access controls	Reduces severity by limiting potential access;	6	Reduces scale by limiting file access
Undetected without controls	240	Application Whitelisting	Decreases likelihood of infection by restricting what software can run	3	Does not decrease severity
Undetected without controls	240	Anti-virus	Decreases likelihood of successful infection;	3	Does not decrease severity
Undetected without controls	240	Role based access controls	Limits access to shared resources reducing potential for malware to spread;	2	Reduces scale of spreading by limiting file share access
Undetected without controls	240	Firewalls	Limits access reducing potential for malware to spread;	2	Reduces scale of spread by limiting network access
Undetected without controls	240	Patches	Decreases likelihood of infection by reducing vulnerabilities	3	Does not decrease severity
Detected due to impact	560	Anti-virus	Increases the likelihood of detecting malware and reduces potential for compromise	7	Reduces scale of impact by halting encryption early in the process
Detected due to impact	560	Backups	Reduces severity of impact by allowing for recovery	5	Does not reduce scale, but allows for recovery
Detected due to impact	560	Role based access controls	Reduces severity by limiting potential access;	9	Reduces scale by limiting file access; however, may still allow for significant encryption
Undetected without controls	350	Application Whitelisting	Decreases likelihood of infection by restricting what software can run	5	Does not decrease severity
Undetected without controls	350	Anti-virus	Decreases likelihood of successful infection; Increases potential to detect successful infections early	5	Does not decrease severity
Undetected without controls	350	Role based access controls	Limits access to shared resources reducing potential for malware to spread; Increase potential for detection through invalid access attempt logging	4	Reduces scale of spreading by limiting file share access
Undetected without controls	350	Firewalls	Limits access reducing potential for malware to spread;	4	Reduces scale o spread by limiting network access
Undetected without controls	350	Patches	Decreases likelihood of infection by reducing vulnerabilities	5	Does not decrease severity

Occ	Occ Reason	Det	Det Reason	RPN	Change
1	Significantly reduces occurrence of non-approved software running	1	Unknown/disapproved attempted executions will be detected	2	198
7	Increases difficulty against known infection vectors	2	Depending on techniques used, execution of malicious code will be detected prior to success	28	172
8	Increases difficulty of email-based infection vectors	3	If malware is delivered via email and uses common/known techniques, it will be detected prior to success	48	152
8	Increases difficulty of open-port based infection vectors	3	If malware attempts to access hosts on disallowed ports or subnets, detection will occur	48	152
9	Slightly increases difficulty based on user/employee awareness levels and technical skills	3	If malware is delivered via a mechanism which involves user interaction and is obvious, it will be detected	54	146
7	Increases difficulty against known infection vectors	10	Does not increase detectability	140	60
9	Does not decrease occurrences	7	Does not increase detectability	126	315
7	Reduces ease of encryption from known threats	4	The encryption process will trigger detection early, due to volume of files affected	168	273
8	Slightly reduces ease of encryption via file shares	6	The encryption process may trigger detection, assuming files protected by RBAC are affected	288	153
1	Significantly reduces occurrence of non-approved software running	1	Unknown/disapproved attempted executions will be detected	3	237
7	Increases difficulty against known infection vectors	2	Depending on techniques used, execution of malicious code will be detected prior to success	42	198
7	Slightly reduces ease of spread via file shares	3	If malware attempts to spread via file shares or other RBAC protected mechanisms, it may be detected	42	198
7	Slightly reduces ease of spread via opened ports	3	If malware attempts to access hosts on disallowed ports or subnets, detection will occur	42	198
7	Increases difficulty against known infection vectors	10	Does not increase detectability	210	30
7	Reduces ease of encryption from known threats	4	The encryption process will trigger detection early, due to volume of files affected	196	364
8	Does not decrease occurrences	7	Does not increase detectability	280	280
7	Slightly reduces ease of encryption via file shares	6	The encryption process may trigger detection, assuming files protected by RBAC are affected	378	182
1	Significantly reduces occurrence of non-approved software running	1	Unknown/disapproved attempted executions will be detected	5	345
6	Increases difficulty against known infection vectors	2	Depending on techniques used, execution of malicious code will be detected prior to success	60	290
6	Slightly reduces ease of spread via file shares	3	If malware attempts to spread via file shares or other RBAC protected mechanisms, it may be detected	72	278
6	Slightly reduces ease of spread via opened ports	3	If malware attempts to access hosts on disallowed ports or subnets, detection will occur	72	278
6	Increases difficulty against known infection vectors	10	Does not increase detectability	300	50

Appendix F – Analysis Techniques: Strengths and Weaknesses

Cyber Modeling Framework Analysis

Strengths

- ✔ Useful in defining the problem, steps, and driving other analysis techniques
- ✔ Useful for identifying solution sets which adhere to defense-in-depth principles
- ✔ Useful for identifying constraints for individual solutions

Weaknesses

- ✗ Produced a large number of solutions with a wide degree of variance
- ✗ Lacked any representation of the effectiveness of costs of each capability
- ✗ Not useful as a stand-alone analysis type

Recommendations Analysis

Strengths

- ✔ Easy to collect and quantify
- ✔ Provides an easy way to collect potential capabilities

Weaknesses

- ✗ Subject to differences in each organization’s criteria
- ✗ Can provide information overload and lacks focus

Failure Mode and Effects Analysis

Strengths

- ✔ Useful for directly comparing capabilities
- ✔ Useful for providing a structured approach to understanding each capability

Weaknesses

- ✗ Subjective based on the analyst’s perspective on each capability’s effect on detectability, impact reduction, and occurrence rates

Subject Matter Expert Commentary Analysis

Strengths

- ✔ Provided a wide variety of positions on each capability

Weaknesses

- ✗ Difficult to review free-form answers
- ✗ Highly subjective analysis

Survey Analysis

Strengths

- ✔ Useful for gaining insight into overall costs
- ✔ Normalizes responses across respondents
- ✔ Easy to quantitatively review

Weaknesses

- ✗ Difficult to create a survey that is not overly complex
- ✗ Sample size may bias results

Real-World Data Review

Strengths

✔ Provides a realistic and objective test for potential solutions

Weaknesses

✗ Subjective decisions on effectiveness

✗ Requires existing data

Strategic Review

Strengths

✔ Easily applied

✔ Provides a good baseline for core criteria

Weaknesses

✗ Not data-driven

✗ Requires a well defined strategy

Appendix G – References

1 https://www.csoonline.com/article/3208111/who-is-a-target-for-ransomware-attacks.html
2 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
3 https://www.securityweek.com/fireeye-predicts-ransomware-will-evolve-and-expand-2021
4 https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time
5 https://www.csoonline.com/article/3385520/how-hackers-use-ransomware-to-hide-data-breaches-and-other-attacks.html
6 https://www.cybersecurity-insiders.com/mamba-ransomware-is-designed-to-cause-destruction-says-kaspersky/
7 https://economictimes.indiatimes.com/markets/stocks/earnings/maze-ransomware-attack-to-hit-cognizant-revenue/articleshow/75251293.cms?from=mdr
8 https://www.mytotalretail.com/article/the-link-between-customer-loyalty-and-ransomware-attacks/
9 https://www.cisecurity.org/white-papers/security-primer-ransomware/
10 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
11 https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
12 https://www.kaspersky.com/blog/cerber-multipurpose-malware/12221/
13 https://www.extremetech.com/internet/303697-ransomware-groups-now-threatening-to-release-stolen-data-if-businesses-dont-pay
14 http://ellis-research.org/cmf.html
15 https://asq.org/quality-resources/fmea
16 https://www.us-cert.gov/ncas/tips/ST19-001
17 https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
18 https://success.trendmicro.com/solution/1112223-ransomware-solutions-best-practice-configuration-and-prevention-using-trend-micro-products
19 https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html
20 https://support.microsoft.com/en-us/help/4013550/windows-protect-your-pc-from-ransomware
21 https://insights.sei.cmu.edu/sei_blog/2017/05/ransomware-best-practices-for-prevention-and-response.html
22 https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/
23 https://www.knowbe4.com/ransomware
24 https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack
25 https://en.wikipedia.org/wiki/CryptoLocker
26 https://en.wikipedia.org/wiki/Locky
27 https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html
28 https://en.wikipedia.org/wiki/Petya_(malware)
29 https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/
30 https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack
31 https://www.avast.com/c-cryptolocker
32 https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/
33 https://en.wikipedia.org/wiki/Petya_(malware)
34 https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html
35 https://en.wikipedia.org/wiki/Petya_(malware)
36 https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/

Appendix G – References

37 https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
38 https://www.avast.com/c-cryptolocker
39 https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/
40 https://en.wikipedia.org/wiki/Petya_(malware)
41 https://en.wikipedia.org/wiki/Petya_(malware)
42 https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/
43 https://www.acalvio.com/wannacry-ransomware-analysis-lateral-movement-propagation/
44 https://www.avast.com/c-cryptolocker
45 https://en.wikipedia.org/wiki/Locky
46 https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/
47 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
48 https://www.securonix.com/securonix-threat-research-samsam-ransomware-detection-using-security-analytics/?PageSpeed=noscript
49 https://www.silverfort.com/blog/how-to-stop-iranian-samsam-hackers-from-taking-your-network-for-ransom/
50 https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack
51 https://www.avast.com/c-cryptolocker
52 https://www.avast.com/c-locky
53 https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper
54 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
55 https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/
56 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
57 https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
58 https://www.avast.com/c-cryptolocker
59 https://en.wikipedia.org/wiki/Locky
60 https://blog.malwarebytes.com/threat-analysis/2016/04/petya-ransomware/
61 https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/
62 https://en.wikipedia.org/wiki/Ransomware#SamSam