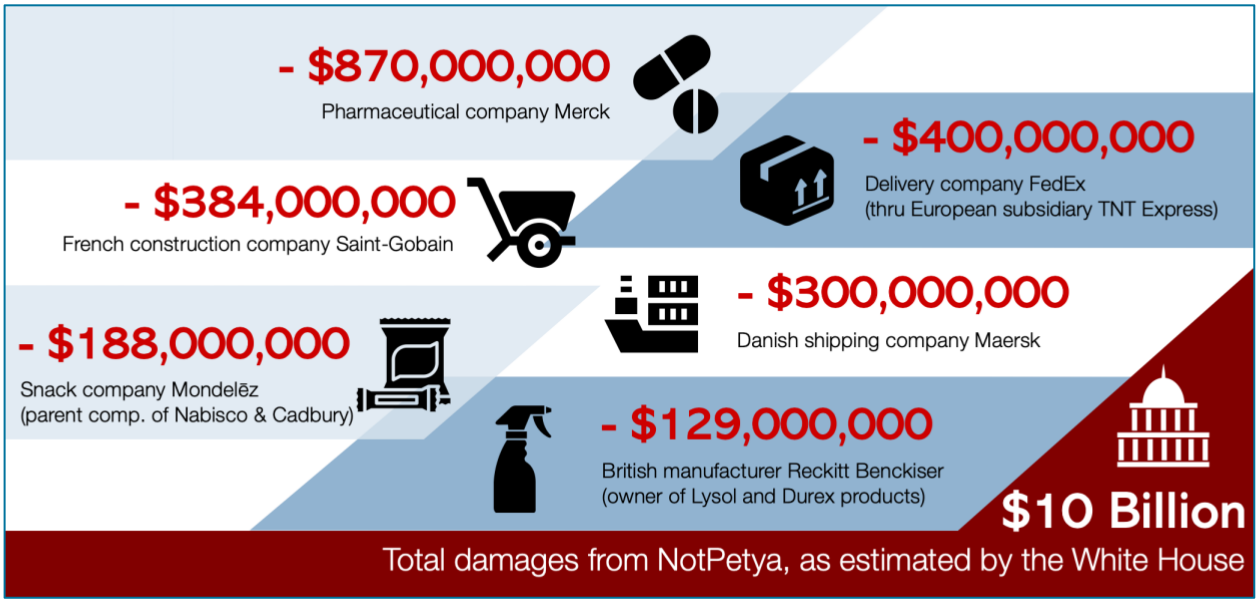
Ransomware Event Modeling

Guidewire Cyence for Cyber Risk Management, Model 4

WHITE PAPER

A *ransom* is a sum of money or other payment demanded or paid for the release of, or access to, a person or asset. In the digital era, where data is considered to be an asset—both the value driver and the foundation of modern business—access to data is a necessity for business operations and therefore becomes an attractive target for cyber criminals. To serve the malicious intent of holding this business necessity—the control and access of data—hostage in exchange for financial gains, the criminal act of ransom is being adopted in the form of ransomware: malicious software (malware) designed to block access to a computer system until a sum of money is paid. Although ransomware has been around for decades, in 2017 it became newsworthy in the global spotlight for causing massive damage and business interruption to the global economy, resulting in losses of billions of dollars.[1]



Source: The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired Magazine, August 2018

Modern-Day Ransomware

You might think that the massive ransomware outbreak of 2017 was long past; ransomware activities and infections have dipped due to better awareness, improved email protection, increased malware blocking, detection efficiency, and other improvements. However, the reality is that ransomware continues to be an even bigger problem for enterprises, as data shows that enterprise infections were up by 12% and accounted for 81% of all ransomware infections, while overall ransomware infections were down in 2018.[2] This shift in victim profile, from consumer to enterprise, is attributed to the mainstream infection paths of ransomware distribution. During 2018, email was the primary attack mechanism for its low- to no-cost, widely adopted, and quick-spread nature. The enterprise segment naturally becomes easy prey because email serves as the chief communication tool. Regardless of a company's size, the malware needs only one point of entry to make a deceptive email the perfect carrier to contaminate an enterprise network. In addition, the result is much more rewarding for extorting a network of people in a business entity rather than individual consumers. Furthermore, most ransomware varieties are designed to target Windows-based computers. Attackers dedicate their focus to the enterprise segment, where the use of Windows devices remains dominant, thereby resulting in a significant uptick in enterprise infection over the past year.

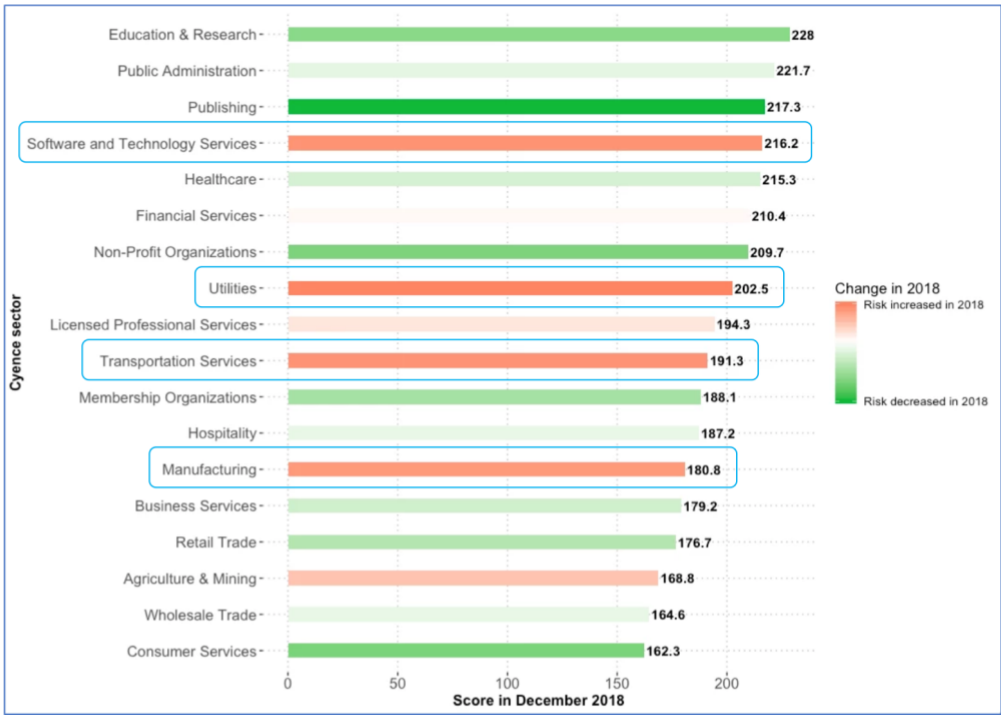
Ransomware criminals have grown more advanced, selective, and concentrated with their attacks. Attackers are looking for higher payouts from selected targets and are opting to buy professional services on the dark web. Sophisticated ransomware criminals are selling custom malware and services that bypass security protections and change when anti-virus software develops counteractive measures. In addition, attackers often use Microsoft

[1] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired* (August 2018).

[2] "Ransomware." *Symantec Internet Security Threat Report* (February 2019).

document or spreadsheet attachments, which are more likely to bypass detection and have a higher chance of being opened. They're also using multiple stages that download the malware in chunks by using built-in Windows commands. By using built-in Windows features, there is more chance that the attacks will evade protections. Once inside the network, many new malware families will spread over the network, looking for important network and database servers to ensure maximum attention and destruction, increasing the chances for a ransom payout.

At Guidewire, our research shows an increase in cyber risk for the technology, utilities, transportation, and manufacturing industries in 2018 in terms of increased data breach risk. This is indicative of a broader risk related to ransomware. After infiltrating networks, attackers have typically two monetization paths: (1) data exfiltration for the purpose of selling private data on the black market, or (2) locking up data to extort the company for a ransom payment. Shortly after we concluded this research, Norsk Hydro (a Swedish aluminum manufacturing giant) experienced a massive ransomware attack that brought the company's computer systems and websites to a halt in March 2019. With Guidewire Cyence™ analytics, we identified ransomware to be a major disruption to business continuity and introduced a new accumulation event for this cyber threat in the fourth generation of our risk model (Model 4) for Guidewire Cyence™ for Cyber Risk Management.

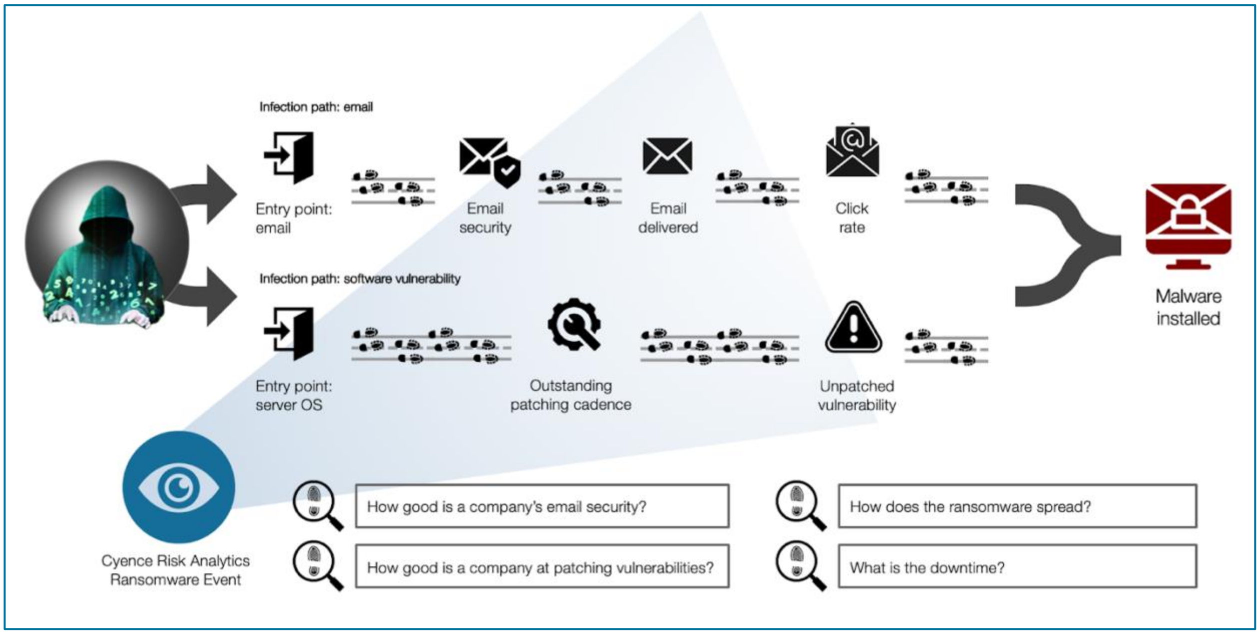


Source: Cyence Risk Analytics internal data

Assessing Ransomware Risk in Model 4

With Model 4, Cyence for Cyber Risk Management expands the parameters of risk evaluation with the addition of an accumulation event for ransomware. This new scenario is designed to estimate loss originating from mass business interruption following a ransomware event. In our scenario, the threat actors are primarily motivated to cause global disruption. Their goal is to share a version of ransomware that is used to gain unauthorized access into a company's network for the broader hacker community. Cyber criminals can easily penetrate a company's network by using this ransomware in phishing campaigns or exploitation of unpatched vulnerabilities. Once in the network, the ransomware locks down data or operating systems to encrypt machines including personal computers, servers to render them unusable. The ransomware is also assumed to have *worming* capabilities, enabling the infection to spread laterally within a company and across multiple companies to cause a widespread business interruption.

Based on our research, email is the most common delivery mechanism for ransomware to attack a company's network. Many sources also indicate that the number of attacks on servers has increased as well.[3] Therefore, the new Cyence ransomware scenario assesses the likelihood of an attack through these two entry points: by email and by exploiting unpatched software vulnerabilities on an externally facing server.


Infection path: email
Entry point: email
Email security
Email delivered
Click rate
Infection path: software vulnerability
Entry point: server OS
Outstanding patching cadence
Unpatched vulnerability
Malware installed
Cyence Risk Analytics Ransomware Event
How good is a company's email security?
How good is a company at patching vulnerabilities?
How does the ransomware spread?
What is the downtime?

The following sections describe how the ransomware scenario uses company-specific data points to quantify ransomware risk. And to further translate risk into dollars and probability, our model is based on the frequency and severity assumptions of the scenario:

- **Frequency assumptions** to identify how many ransomware events are likely triggered and which companies are affected
- **Severity assumptions** to determine the spread of the malware following an attack and to help estimate the downtime caused by the malware when it spreads to additional business interruption losses

With these assumptions, Cyence for Cyber Risk Management runs Monte Carlo simulations to provide a stochastic view of the ransomware scenario. The following sections describe the assumptions in detail.

Frequency

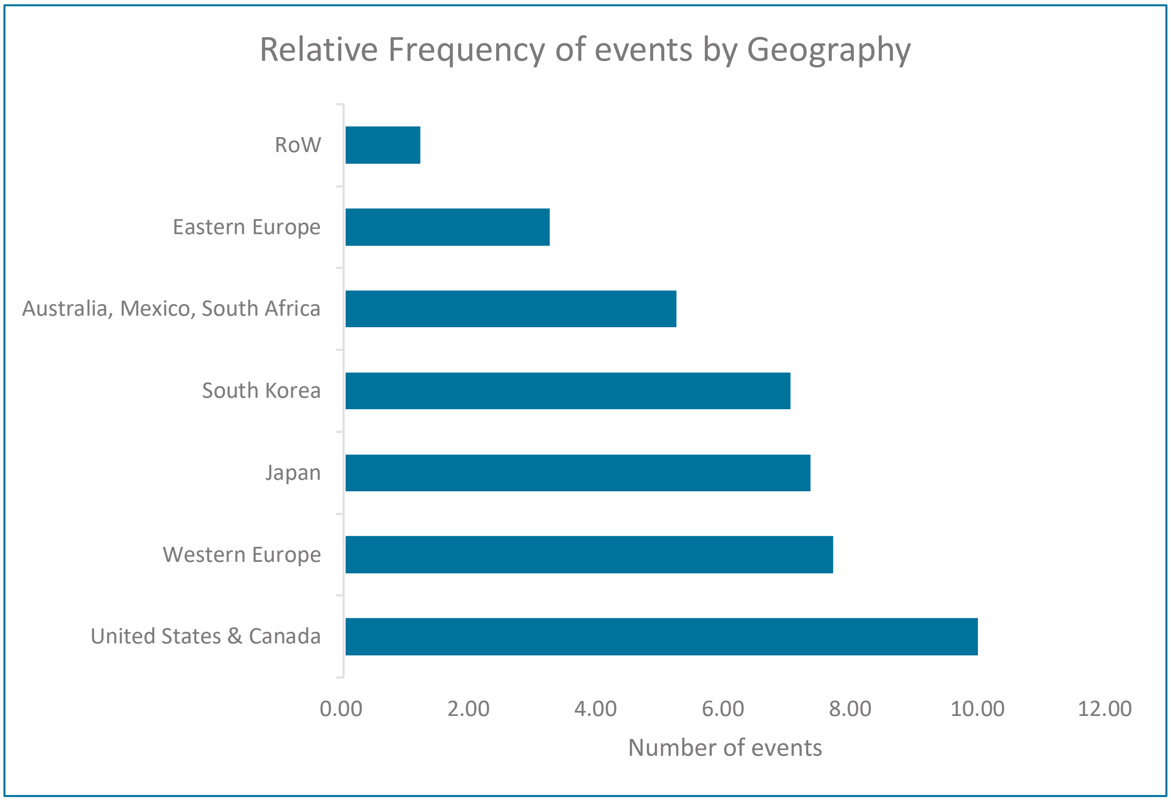
Step 1: Quantify the number of ransomware attacks.

The scenario that Guidewire Cyence is modeling is a case of accumulation ransomware. This means that multiple companies will be affected as a result of the same event. The first step, therefore, is to estimate the number of massive ransomware events likely to occur over the next 12 months. In the past 10 years, hacker groups such as the Shadow Brokers deliberately orchestrated approximately five major leaks of sensitive information that exposed enterprise software vulnerabilities and exploits out in the open.[4] This information was later used by cyber criminals for malicious attacks, many of which proved to be severe at a global scale. For example, the release of EternalBlue was ultimately used to conduct WannaCry, which caused billions of dollars in monetary losses to the global economy. Based on these historical events and the expert opinions of the Cyence cybersecurity team, we project that four such events may happen over the next 10 years.

[3] *Advisen Data Breach Report* (2018)

[4] "The 18 Biggest Data Breaches of the 21st Century." *CSO Magazine* (December 2018).

In terms of the ransomware landscape, the attacks are not evenly distributed across the globe. Based on research, we assume that risk in certain countries is higher than in others.[5] The following table shows relative risk assumed in our ransomware scenario.



For every 10 ransomware events in United States, there are approximately 8 events in Western Europe

Western Europe includes United Kingdom, Germany, Denmark, France, Ireland, Italy, Netherlands, Norway, Spain, Portugal etc.
Eastern Europe includes Belarus, Bulgaria, Slovakia, Ukraine, Poland etc.
RoW includes Middle East, South East Asia, Africa, South America

Source: Cyence Risk Analytics internal data

For every 10 attacks targeting the Unites States, about eight events target Western Europe. Our experts believe that the U.S. will continue to have the highest risk for three main reasons:

- The GDP per capita is higher in the U.S. compared to other parts of the world. Whether the hackers are seeking financial extortion or causing disruption, targeting the U.S. would presumably cause the most damage for the least amount of effort.
- Data from the U.S. (such as PII, PCI, and PHI) is of higher value to hackers than in other countries.
- The U.S. and Canada both have English as a common language. This allows attackers to cast a wider net for ransomware campaigns. Regions like Europe and Asia, where languages are highly diverse, would constrain hackers to either launch a narrower campaign or overcome the nuances and cultural differences of people in different countries.

[5] "Ransomware: Holding Your Data Hostage." *Deloitte Threat Intelligence and Analytics* (2016)

Step 2: Identify the impacted companies after ransomware attacks.

Now that we have the number of events, we next want to identify the impacted companies. To do this, we consider two major factors: the geography of the companies and their subsidiaries, and their security posture including email security, patching cadence, and so on.

Geography

The Cyence risk model looks at the locations of not only the parent company but also subsidiaries to gain a holistic view of whether a company will be impacted. For example, Acme Corporation is headquartered in the United States but has subsidiaries that operate in Europe. Acme will be exposed to ransomware attacks targeted in both geographies. This means that companies with headquarters and operating subsidiaries in multiple geographies are exposed to increased attack vectors and suffer a higher likelihood of being impacted by a ransomware attack.

Security Posture

In addition to geography, the risk model uses idiosyncratic company attributes to adjust the likelihood that a company will be attacked and ultimately suffer a loss. The following sections describe this process according to each infection path.

Infection Path: Email

To determine whether a company is likely to be a victim of a successful ransomware attack, a useful metric is to identify the likelihood that someone in the company's network will perform the following actions:

1. Open a phishing email.
2. Click a malicious link in the message or download a malicious attachment.

Such actions would trigger events including installation of malware, machine encryption, and lateral spreading. As a result, the model looks at and normalizes results from multiple industry studies to identify the likelihood that someone would open a phishing email and perform actions that have a malicious intent.

Because companies have different security postures, the model looks at company specific data points about email security that would either increase or decrease the likelihood of an email message being successfully delivered to an inbox and potentially opened. One of the metrics we use is evaluating the configuration of the Sender Policy Framework (SPF), which can identify spoofing or phishing emails. If data shows that the SPF is misconfigured, we increase the likelihood that a phishing email would be successfully delivered to a company's inbox and subsequently clicked.

Infection Path: Compromised Servers

Ransomware can also be delivered by exploiting the software vulnerability of an external-facing server. Companies without external-facing servers are not exposed to this infection path. However, for companies running an operating system on an external-facing server, the Cyence model is able to pick up this information and identify these companies as potential targets of the infection path.

This attack vector focuses on the two most common server operating systems: Windows and Linux.[6] The scenario assumes that there may be unpatched vulnerabilities on these operating systems that can be exploited for malware delivery. The model analyzes a company's patching cadence and tracks how often the company remediates its unpatched vulnerabilities. Companies with a slow patching cadence have a higher likelihood of ransomware penetration through server vulnerability. In contrast, we assume the chance of ransomware penetration is significantly lower if a company's IT team has a scrutinized patching cadence that resolves system vulnerability in a timely manner.

[6] *Market Share Analysis: Server Operating Systems, Worldwide, 2015*. Gartner (May 2016).

Severity

Many hackers operate with the sole motivation of causing disruption. For this reason, when a ransomware event is under way and the hacker demands an extortion payment, the ransom payment by itself does not guarantee that the interruption will stop.

To account for all possibilities, the scenario estimates business losses from the following two coverage parts:

- **Business interruption:** Business income loss and extra expenses
- **Cyber extortion:** Extortion payments and forensics

Coverage Part: Business Interruption

To determine business income loss, we need to quantify the magnitude of disruption caused by a particular ransomware attack. A good metric is estimating downtime—the time required for a business to return to normal operations following a ransomware attack—and then quantifying the resulting business income loss.

Cyence defines business interruption loss with the following formula:

Business Interruption Loss = Business Recovery Duration × Business Dependency × Income and Extra Expenses

For *business recovery duration*, the focus is on estimating the downtime, which we calculate by closely examining the following two components:

- Time needed to fix, re-image the affected machines, restore backups, and so on
- Time needed to return to normal operations (that is, clearing backlogs)

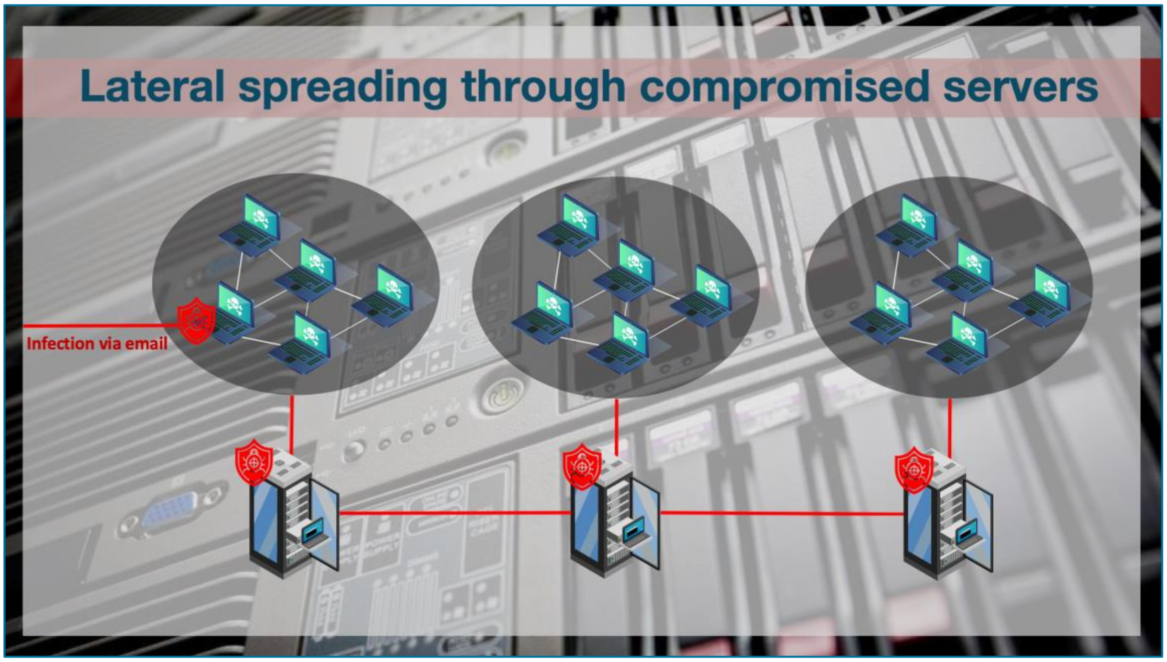
Time Needed to Fix the Affected Machines and Recover Data

When a company is dealing with a ransomware attack, the first order of operations is usually to decrypt the machines or wipe them clean by reimaging to factory settings and restoring backups. To determine how much time is needed to complete this process, the risk model considers the following factors:

- Size of the company
- Network segmentation
- Size of the IT department

To estimate the time needed to clean and reimage machines after an attack, we first look at the size of the company to determine the breadth of the impact. Then we look at how well the company's network is segmented to determine the depth of lateral spreading. Network segmentation is a common practice to improve performance and increase security. If a network is segmented well and has a timely patching cadence, the spread of the ransomware and the business damage can be easily contained. On the other hand, if the servers have unpatched vulnerabilities, the likelihood for an infection to easily spread across servers is higher. By factoring in the breadth (company size) and depth (lateral spreading capability) of impact, our model can estimate the number of impacted endpoints.

After most attacks, IT teams work overtime and long hours to contain damage and return to normal operations. Therefore, it's essential to consider the size of the IT organization when estimating the recovery time. The model estimates the size of an IT department based on the company's revenue and employee count. For each IT employee, the model assumes that approximately three endpoints can be fixed or re-imaged each day based on normalized data collected from various industries. As a result, we're able to assess downtime for repair by dividing the estimated number of impacted endpoints by the projected size of the IT department and each IT worker's daily repair rate. For example, if an IT department of 20 is responsible for the repair of 480 impact endpoints, the total repair time consumed by IT would be 8 days, calculated by dividing 480 endpoints by 20 workers and 3 repairs per person per day (480 ÷ 20 ÷ 3 = 8 days).



Time Needed to Return to Normal Operations

After machines are repaired and data is restored, the last step in recovery is to clear the backlog that was created as a result of the interruption. The extent of backlog can vary based on industries and lines of work. For example, a ransomware attack at an airline can cause massive flight cancellations that lead to a severe backlog after a return to normal operations. This includes the fulfillment of canceled flights and associated incurred expenses such as employee overtime. Manufacturers can suffer from a similar impact if they are unable to fulfill orders causing a domino impact to the downstream supply chain. From a severity standpoint, transportation, logistics, and manufacturing with global operations face far higher likelihood of lengthy downtime and recovery than other industries with only domestic operations. Cyence takes this phenomenon into account by further adjusting the estimated downtime based on the industry and the number of geographies a company operates in.

For *business dependency*, the level of technology dependency varies across industries. Some companies can continue business operations despite undergoing a ransomware attack. The Cyence ransomware scenario assumes that each company remains partially operational during the downtime and slowly returns to normal operations in the next four to eight weeks.

Coverage Part: Cyber Extortion

Hackers demand a ransom payment determined by the number of encrypted endpoints (laptops, servers, and other hardware). Based on historical incidents, our risk model estimates that the approximate ransom demand is between $600 and $700 per encrypted endpoint.[7]

The scenario assumes that one-third of all successful ransomware events result in payments made to attackers.[8] This conclusion is based on researching past ransomware events in an industry. Unfortunately, because attackers' intentions can be purely malicious, with the sole purpose of causing disruption, we cannot assume that an attack has ended or that the hackers will provide an encryption key after receiving the extortion payments. This means that business interruption losses should be anticipated regardless of whether the ransom is paid.

[7] "Average Ransomware Payment Rose 13% to $6,700 in Q4 2018 from Q3." *Business Insights* (February 2019).

[8] "27 Terrifying Ransomware Statistics & Facts You Need to Read." phoenixNAP Global IT Services Blog (January 2019).

Forensic investigation is also a critical cost component. A company's IT staff typically works alongside contracted third-party vendors on a thorough analysis to determine the exact nature of what happened, the extent of the attack, and whether data was breached.[9] At times, companies may have pre-negotiated rates for forensics, which may lower their expected cost. The Cyence ransomware scenario estimates a forensic expense of $24,000 for each week of downtime.

Looking Ahead

In recent years, ransomware has severely plagued the global economy. Enterprise IT security has responded to this challenge with better parameter security, detection mechanisms, and staff training for increased awareness. However, insurers are slow to react because they lack of dedicated analytical solutions to translate this cyber risk into probability and financial measures.

With the fourth-generation model update for Cyence for Cyber Risk Management, Guidewire is introducing advanced analytics modeling for ransomware to reflect the evolving cyber landscape. This advancement expands the parameters of risk evaluation by incorporating the likelihood of a ransomware attack into the broader cyber risk model. By having a comprehensive view of cyber risk exposure, insurers can improve their portfolio exposure management, set appropriate limits, and gain the confidence to adapt and succeed in this fast-changing environment.

For additional information, contact your local Guidewire sales representative or visit https://www.guidewire.com/contact-us.

About Guidewire Software

Guidewire delivers the industry platform that Property and Casualty (P&C) insurers rely upon to adapt and succeed in a time of accelerating change. We provide the software, services, and partner ecosystem to enable our customers to run, differentiate, and grow their business. We are privileged to serve more than 350 companies in 40 countries. For more information, please visit www.guidewire.com and follow us on twitter: @Guidewire_PandC.

[9] For the purpose of this scenario, the Cyence risk model assumes that no data was breached and therefore the company does not have notification requirements. This scenario was designed to estimate a mass global business interruption. For details about quantification of loss following a mass data breach, refer to the Cyence zero-day vulnerability scenario.