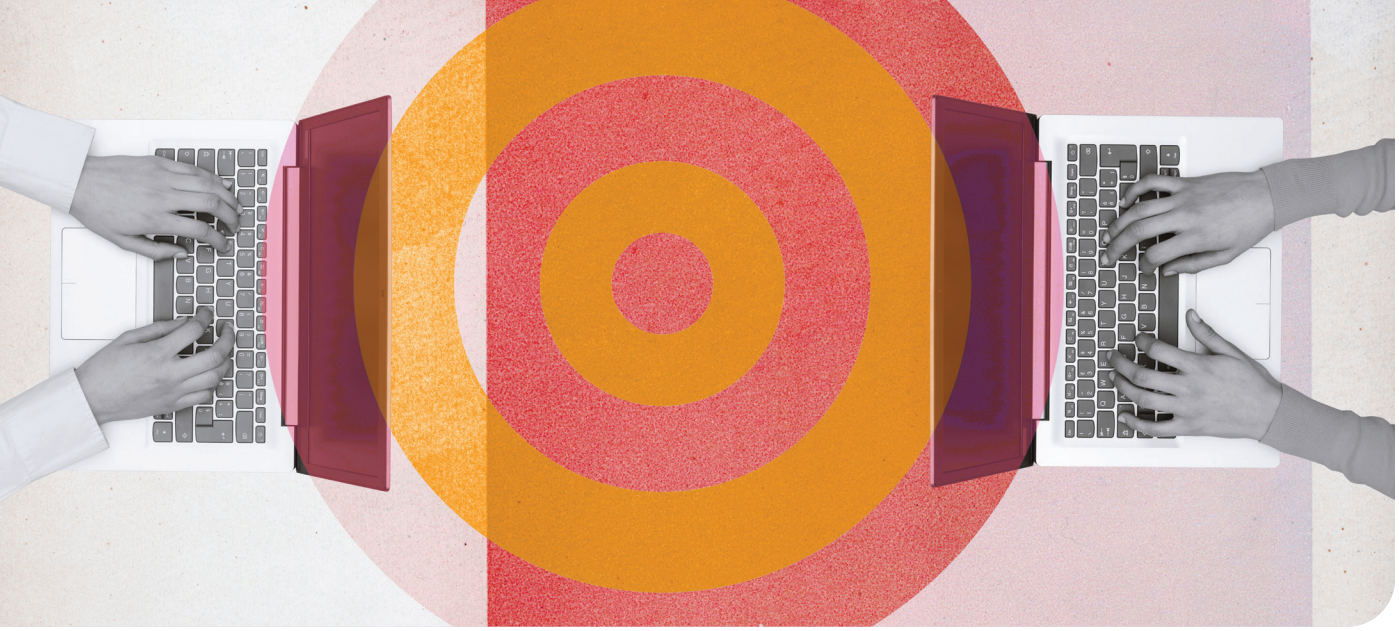
halcyon

What Executives Should Know About Ransomware

Educating executive leaders on mitigating the risks of ransomware in the digital era



01 What Executives Should Know About Ransomware

In today's digital age, businesses have become entirely reliant on technology to streamline operations, enhance productivity, and connect with customers. While these advancements have undoubtedly brought numerous benefits, they have also opened the door to a growing threat: ransomware attacks.

The cost to victims from ransomware attacks is estimated to reach $265 billion (USD) annually by 2031. The rapid growth of ransomware attacks has made this cyber threat a top concern for businesses and organizations worldwide. The volume of attacks surged in 2023 by 55.5% year-over-year, with 4,368 cases documented cases, with only a fraction of all attacks being reported.

As an executive, it is crucial to understand the potential impact of disruptive cyber-attacks on your business and take proactive steps to mitigate them. In the past few years, the role of the CISO has seen increased scrutiny as some in the role have faced legal challenges as data loss associated with ransomware attacks have continued to impact large organizations and their customer base.

In this reference guide, we'll explore what each C-level executive should know about ransomware in order to ensure a strong security posture and protect their organization.

The cost to victims from ransomware attacks is set to reach $265 billion (USD) annually by 2031.

Understanding Ransomware Attacks

Ransomware is a type of malicious software that encrypts a victim's data and systems, rendering them inaccessible. Perpetrators demand a ransom payment, typically in cryptocurrency, in exchange for a decryption key that will

unlock the systems and data. The threat actors behind these attacks are often well-organized, technologically adept, and motivated by financial gain.

Ransomware is fundamentally different from other forms of malware as the goal is to be disruptive to an organization, as opposed to remaining undetected. Current investments in cybersecurity are often not focused on the unique aspects of the ransomware threat.

Ransomware is no longer considered a boutique threat, but rather one of the most significant threats to any organization. The vast majority (75%) of organizations reported being targeted by at least one ransomware attack in 2023, with 26% reporting they were targeted with ransomware four or more times.

The vast majority (75%) of organizations reported being targeted by at least one ransomware attack in 2023.

Current endpoint protection solutions available on the market, while robust and effective for many threats, do not fully protect against ransomware attacks because they were designed to find and block commodity malware.

Ransomware-as-a-Service (RaaS) operators and data extortion attackers are implementing novel evasion techniques into their payloads designed to completely circumvent traditional endpoint protection solutions.

Understanding how ransomware works and the specific responsibilities of each executive can help mitigate the risks and ensure your organization remains secure.

Evolving Ransomware Threat Landscape

The rise of RaaS operators mimics the more conventional Software-as-a-Service (SaaS) business model by every meaningful measure. The ransomware economy involves multiple players who specialize in various aspects of the larger ransomware attack, each taking a cut of the proceeds.

The overall maturity, level of organization, and specialization within the ransomware economy means we are dealing with an adversary whose tactics, techniques, and procedures (TTPs) are approaching the sophistication of some nation-state-sponsored attackers.

In many cases, there has been documented overlap between nation-state attack elements and those of cybercriminal ransomware gangs. Today's ransomware attacks are more complex and difficult to defend against than ever before.

Make no mistake, ransomware is big business, and the ransomware game is extremely profitable. In fact, if you were to compare P&L sheets from the leading ransomware operations against leading security solution providers, you'd see ransomware gangs enjoy operating margins that would make almost any SaaS provider envious.

Ransomware operators are better viewed as mature criminal business organizations with top-down hierarchical structures and diversified revenue streams. They employ various tactics, such as spear-phishing, social engineering, and exploiting software vulnerabilities. CXOs must understand that ransomware is not a one-time risk factor, but an ongoing, adaptive threat.

Attackers are getting more efficient at exploiting vulnerabilities, and this trend is likely to continue as threat actors automate aspects of their attack sequences. We see evidence of this automation in the thousands of organizations that have been hit by just one ransomware group exploiting one patchable vulnerability in early 2023.

Nowhere is this more evident than in the continued exploitation of a vulnerability in the MOVEit managed file transfer software (CVE-2023-34362) the CIOp ransomware gang has leveraged to compromise more than 1000 victims in rapid succession in a matter of weeks.

The wave of attacks followed another earlier in the year where threat actors successfully compromised more than a hundred targets by exploiting a patchable bug in the GoAnywhere file transfer tool (CVE-2023-0669).

Overall, the marked increase in the exploitation of vulnerabilities by ransomware gangs is evidence that criminal actors are increasingly using more complex tactics usually seen in state-supported operations versus the random 'spray and pray' ransomware attacks of the past. This mass exploitation wave is also evidence that ransomware gangs are increasingly leveraging automation to identify and target exposed organizations who have not patched against known vulnerabilities, which is why we are seeing so many new victims.

The bad news is that as attackers are getting more proficient at automating aspects of the attack progression by exploiting known vulnerabilities for initial access, improving stealthy payload delivery, fine tuning evasion techniques, and exponentially improving encryption speeds, we will likely continue to see an escalation in the volume and severity of attacks.

The good news is that, given that these attacks leverage exploits for well-documented vulnerabilities, we can detect and stop these ransomware operations earlier in the attack sequence. Many of the TTPs they employ are common and should help to reveal a host of detectable activity on the network that occurs long before the actual ransomware payload is delivered.

Organizations with the right controls in place stand a good chance of disrupting these attacks at initial ingress when these known exploits are likely to be used, or when the attackers begin to move laterally on the network and seek to escalate privileges. The ransomware payload is the very tail-end of a longer attack, so a multi-layer defense strategy that is designed to detect more than just the detonation of a ransomware binary is critical to detecting earlier and remediating against these attacks faster.

Financial Losses and Liabilities from Ransomware Attacks

One of the most immediate concerns for CXOs regarding ransomware attacks is the financial impact on the business. The ransom demands can range from thousands to tens of millions of dollars, and there are additional costs associated with incident response, legal counsel, and potentially even regulatory fines.

On average, a ransomware attack took 237 days to detect and 89 days to fully remediate (PDF). The annual impact from ransomware attacks in the US alone is estimated to be more than $20 billion dollars. Remediation costs following a ransomware attack average more than $4M per incident per each targeted organization.

This figure does not include additional incident response costs, tangential costs, damage to the brand, lost revenue, lost production from downed systems, and other collateral damage:

Intellectual Property and Regulated Data Loss: After an attacker successfully executes their attack, they do not simply deny access to your data – they will send that data outside of your network and threaten to leak it publicly. For many organizations this exposure of customer data has regulatory implications and can lead to lawsuits and fines. Additionally, sensitive data on corporate transactions, patents, etc. can end up in the attackers' hands and be sold to the highest bidder on dark web forums.

Incident Response and Remediation Costs: The average incident response cost for a ransomware attack is $4.54 million, more than the average cost of a data breach, which is $4.35 million. While larger organizations can absorb these costs, this potentially represents an existential threat to smaller companies.

Tangential Costs to the Business: The above figures did not even include the ransom payment, the long-term damage to an organizations' brand (loss of consumer trust), increased cyber insurance premiums, legal fees, or lost revenue which can far exceed remediation costs – this is why the focus needs to be on both prevention and resilience. These losses are nearly impossible for an organization to forecast and budget for, and in some cases can represent an existential crisis for smaller organizations.

Moreover, paying the ransom is not guaranteed to result in data recovery. In fact, experts advise against paying ransoms, as it incentivizes the criminal enterprise and does not guarantee the safe return of your data.

Current trends indicate that ransomware operators are taking advantage of the potential for multiple opportunities for revenue from an attack not only from the initial target, but potentially from partners, vendors, customers, and other third-party entities that could find themselves the victims of extortion by way of data compromised in the initial attack.

This further complicates the decision to pay a ransom, will the payoff mitigate the exposure to the extent required? CXOs must weigh all potential impact, financial losses, and costs associated with recovery against the decision to pay or not.

Ransom Demands: To Pay or Not to Pay

In recent years, the debate on whether to pay ransom demands or not has become a contentious issue among experts. The simple answer would seem to be that organizations should never pay a ransom demand, which would significantly diminish the financial incentives for these attacks.

In most circumstances that would be the logical approach, but it may not be the right approach for every organization. For example, it may be within the risk parameters for a retailer to refuse a ransom demand even though downtime is costing the organization revenue while recovery efforts are underway.

But what about a hospital who urgently requires access to systems where any delays could pose a risk to human life? In these cases, the decision on whether to pay a ransom demand is more complicated. This is why experts are divided on whether organizations should pay ransomware demands.

Those who advocate for paying the ransom believe that it's the quickest and easiest way to regain access to valuable data and is the best way to reduce the overall impact of an attack. They argue that the cost of paying the ransom is often lower than the cost of restoring data from backups or the potential financial losses incurred from delayed recovery.

On the other hand, those who oppose paying the ransom argue that doing so only encourages cybercriminals to continue their attacks by reinforcing the financial incentives that drive ransomware attacks. They point to examples where paying the ransom did not guarantee that the victim's data was restored or cases where the data was corrupted during decryption.

They also point out that most victims who paid a ransom demand were attacked again, often by the same threat actor who demands a higher ransom payment knowing the victim is likely to pay.

> Most victims who paid a ransom demand were attacked again.

While paying the ransom may seem like a quick fix, it may not be the best solution for businesses and individuals. Paying the ransom only supports the criminal activities of cybercriminals, leading to an increase in ransomware attacks. Additionally, paying the ransom does not guarantee that the victim's data will be restored.

There have been instances where victims have paid the ransom, but the cybercriminals did not provide the decryption key or provided a faulty one, leaving the victim without their data and their money. Also, even if the victim's data is restored, paying the ransom may result in further attacks. Cybercriminals may see the victim as an easy target and continue to target them with future attacks.

Finally, paying the ransom does not address the root cause of the problem, which is the vulnerability of the victim's network to ransomware attacks. Instead of paying the ransom, victims should focus on implementing preventative measures to protect their data from future attacks.

Organizations need to consider the specific dynamics of the attack, the specifics of the systems compromised, and the nature of the business itself.

The optimal time to have these discussions is prior to an event. Potential scenarios need to be run through before they are actual events to enable leaders to examine the factors in play and develop the right strategies for when an event occurs.

Operational Disruptions

Ransomware attacks can bring a business to a grinding halt. When critical systems and data are locked, daily operations are severely disrupted. This can lead to lost revenue, missed opportunities, and damage to the company's reputation. In some cases, businesses are forced to shut down temporarily, which can have lasting repercussions.

For example, in May of 2023, a manufacturing company with revenues nearing $1B annually was attacked by the Akira ransomware group. Akira encrypted all Windows workstations and servers halting their business and operations. All backups were destroyed and were not recoverable.

Not only was the company almost completely unable to conduct business or proceed with production, but the company also faced the unpleasant reality that they would need to rebuild all their systems from scratch which would require multiple technology partners and take months to complete at great cost to the organization.

While some larger companies can weather disruption like this, it may be an existential event for most small to medium organizations who may not have the resources required to spend weeks getting systems back up and running.

To mitigate operational disruptions, CXOs should ensure robust backup and disaster recovery plans are in place. Regular testing of these plans is vital to ensure data can be restored quickly and efficiently in an attack.

Data and Intellectual Property Loss

Beyond the financial and operational impact, CXOs should also be concerned about the potential loss of sensitive data and intellectual property. Ransomware attackers often threaten to publish or sell stolen data if the ransom is not paid. This can lead to regulatory fines, legal liabilities, and severe damage to the company's brand and customer trust.

Protecting sensitive data through robust cybersecurity measures, including encryption, access controls, and employee training, is essential in safeguarding against data loss and intellectual property theft.

Data exfiltration and the threat of exposure are now a central aspect of nearly every ransomware operator's playbook and significantly increase the chances for the extortion efforts to be successful.

The Double Extortion tactic begins when they exfiltrate sensitive information from the target before launching the encryption routine. The threat actor then makes the additional demand that victims pay up to prevent the attackers from publishing their data online.

We see this most clearly in the evolution of the extortion tactics employed by the ransomware actors. Originally, the malicious payloads would encrypt files and demand payment for decryption keys. Security teams found success in either restoring from backups or accepting loss of data as an acceptable consequence.

In some cases, the attackers may not only demand payment of a ransom to regain access to encrypted systems, but they may also demand further payment for the stolen data itself. Of course, there is no guarantee that payment will protect the stolen data from being exploited.

CXOs need to understand that today's ransomware attacks involve a great deal more than just the delivery of malicious code and the issuing of a ransom demand. Data exfiltration is central to nearly every major ransomware operation, and the tactic has been so successful that some groups have abandoned the encryption aspect of attacks altogether to focus solely on stealing data and extorting the victim.

Brand and Reputational Damage

A company's brand is one of its most valuable assets. Ransomware attacks can tarnish this reputation, eroding customer trust and loyalty. News of a data breach or ransomware incident can spread quickly, causing reputational damage that may take years to repair.

According to one study, 75 percent of customers would consider switching brands following a ransomware attack. While that figure may seem high, even if it were halved there are not many businesses who would see the potential loss of one-third of their customers due to an attack as an acceptable risk.

75% of customers would consider switching brands following a ransomware attack.

To mitigate reputational damage, CXOs should communicate openly and transparently with stakeholders, customers, and the public in the event of an attack. Establishing a crisis communication plan and actively managing the company's response can help mitigate the long-term impact on reputation.

Legal and Regulatory Consequences

For many organizations, this exposure of customer data has regulatory implications and can lead to lawsuits and fines. Additionally, sensitive data on corporate transactions, patents, etc. can end up in the attackers' hands and be sold to the highest bidder on dark web forums.

Ransomware attacks often trigger legal and regulatory consequences. Depending on your industry and location, there may be data protection laws and regulations that require you to report data breaches promptly. Failure to do so can result in substantial fines and legal liabilities.

Most ransomware attacks today include data exfiltration prior to the encryption of systems. The stolen data is used as leverage to compel the victim to pay the ransom demand with the threat of releasing or otherwise exposing the data if payment is not made.

Even if organizations are prepared to respond and recover from a ransomware attack, the fact that sensitive data was stolen or exposed puts them at additional liability risk. The number of class action lawsuits spurred by ransomware attacks that include data exfiltration has skyrocketed in the last two years, and the liability risk is also specifically hitting the C-suite and Boards of Directors.

To navigate this landscape, CXOs should work closely with legal counsel to understand their obligations and develop a proactive approach to compliance. Additionally, investing in cybersecurity measures that align with industry standards and regulations is crucial for avoiding legal repercussions.

Cyber Insurance

There are so many issues around how best to approach insuring against losses stemming from cyberattacks; it's a difficult subject to encapsulate, especially regarding coverage for ransomware attacks.

On the macro level, it's about accurately quantifying risk in an area where the risk factor is constantly changing as threat actors innovate, improve their capabilities, and mature their platforms.

As it stands, insurance companies have not been able to put their finger on the magic equation that allows for affordable policies for both the insured and the insurer. Ransomware attacks vary in severity, and ransom demands range from tens of thousands to tens of millions of dollars.

Furthermore, organizations may handle different kinds of sensitive data that put them in different liability categories, and they may use a wide range of security solutions, each filling one small gap in protection, all of which need to work together to prevent a disruptive event. This is a complicated ecosystem for insurers to cover.

Then there is the issue of compliance with the terms of the cyber insurance policy. If an organization practices a check box approach to security compliance, they may have all the boxes checked as far as the required controls being in place, but they may be surprised to find that a claim is denied because of common issues like misconfigurations or the inability to patch against vulnerabilities in a timely manner.

Then there is the data exfiltration issue; most ransomware attacks today include data exfiltration prior to the encryption of systems. The kind of data that was compromised can be a major variable in potential losses to the victim organization.

Regulated data like personally identifiable information (PII) can be especially problematic from a liability perspective, and we are seeing more and more lawsuits following data loss events associated with ransomware attacks.

Then there is the threat of losing intellectual property that could impact the viability and competitiveness in the market of a business, which is extremely hard to quantify, so likely not covered by cyber insurance policies.

In short, customers are facing more restrictive policies with add-ons for covering ransomware-related losses, more comprehensive audits of security controls, and ever-increasing premiums, while insurance providers are facing a crunch on pricing the policies accurately to cover the losses they see in the real-world, which are continuing to grow.

More focus needs to be placed "left of boom" - at initial ingress, command and control (C2), lateral movement, data exfiltration, and so on. If we are doing our jobs right, and stop an attack at these earlier stages, then we would not even know it was a ransomware attack, just another run-of-mill intrusion event.

As well, there is not enough focus on what comes after "boom" - how the organization can plan for the failure of security controls and be positioned to respond efficiently and effectively to a future ransomware attack, making the organization and its operations as resilient as possible by reducing the potential for mass disruption.

Detecting and blocking the ransomware payload is really important, but we know we can't be 100% on this, so if we put more emphasis on detecting and blocking what comes before the ransomware as well as putting a focus on what steps to take after infection, this will go a long way to better quantifying risks and stabilize the very volatile cyber insurance market.

SEC Reporting Requirements

The U.S. Securities and Exchange Commission (SEC) now requires publicly traded companies to disclose cyberattack events within four business days if they are deemed "material" to current and prospective shareholders "in making an investment decision."

It's a no-brainer that more visibility and accountability regarding security-related events at publicly traded companies is a good thing. However, we must be careful not to confuse disclosing information about a cyberattack with informing investors about why an attack should be considered in their investment decisions.

The fact is publicly traded companies are targeted and attacked daily.

The fact is publicly traded companies are targeted and attacked every day. And large companies may be attacked hundreds of times in a single day. As we in the security trade already know, you can't stop cyberattacks, but you can stop an attack from being successful and attaining its intended objective.

That said, the real challenge with this new SEC ruleset will be twofold: first, the onus is on corporate officers to decide if and when a security event reaches the threshold of being "material" to investors. This leaves quite a bit of room for subjectivity, plausible deniability, and – if not structured correctly – could produce a culture where there is pressure on security teams to conceal security events from the executive suite, to keep the event unreported.

The second challenge is whether investors are educated enough about cyber to know what to do with information about an incident – and this is the real rub here. A significant amount of time can pass between "we are under attack" and "we understand the full nature of and potential impact of the attack." Forensic investigations are difficult and take time.

The disclosure rule set by the SEC, if not supported by investor education efforts, has the potential to create a situation where an attack is disclosed but the details are murky because it could be weeks or months before the organization can adequately assess the information the SEC is requiring be reported. But once investors are informed of an attack, they will want the details, and want them immediately.

This could create situations where company leadership appears incompetent because they can't answer tough questions about an event, undermining investor confidence. Furthermore, the company's leadership would be put in a position where they trickle out incomplete information over time as the investigation progresses and simply end up dying by a thousand cuts. This inability to provide concrete answers immediately will likely create confusion and anxiety for investors, causing them to overreact to an event that - while reportable per SEC rules – may not be that serious of an event from a security standpoint.

Any requirements on victim organizations to report material security events to investors must come with a concerted effort to educate investors on the nuances of attacks, security operations, and risk, or the SEC will create more problems than they are actually solving.

Defending Against Ransomware Attacks

The attacks targeting organizations for large ransom payouts today are complex multi-stage operations, and the ransomware payload is typically at the tail-end of the longer attack sequence This means there are typically weeks or even months of detectable activity on the network that occurs before the data and systems are rendered inaccessible and a ransom demand is issued.
A robust ransomware defense begins with assuring the organization has the basics down. The following are controls and procedures every organization should implement even when not taking the threat of an attack into consideration to establish a steadfast, baseline security posture:

Patch Management

Keep all software and operating systems up to date and patched.

Data backups

Assure critical data is backed up off-site and protected from corruption in the case of a ransomware attack.

Access Control

Implement network segmentation and policies of least privilege (Zero Trust).

Awareness

Implement an employee awareness program to educate against risky behaviors, phishing techniques, etc.

Procedure Testing

Plan and prepare for failure by running regular tabletop exercises and ensuring all stakeholders are ready to respond to an attack.

Resilience Testing

Test solutions against simulated ransomware attacks to assure detection, prevention, response, and full recovery of targeted systems.

Basic security hygiene is not enough though. Most attacks start at the endpoint, so endpoint security and resiliency are essential. Let's take a deeper look at the evolution of endpoint protection, the tools available, and where they fall short in defending against ransomware attacks.

ENDPOINT SECURITY

The concept of endpoint security is simple: protect endpoints like servers and end-user devices like desktops, laptops, tablets, mobile devices, and more from unauthorized access and exploitation. The practice of defending endpoints effectively? That is far from easy. The security industry continues to evolve means and methods for improving endpoint security – the following is a rundown of the last 40 years of endpoint security product evolution:

FIREWALLS

The most basic is a software-based firewall software for endpoint devices, which is designed to regulate traffic to the endpoint it is installed on and prevent malicious interactions and some unauthorized installations. But firewalls, while important, are easy to bypass and have limited utility, so in addition, organizations deploy a traditional (AV) or next-generation antivirus (NGAV) is highly recommended.

TRADITIONAL ANTIVIRUS (AV)

If kept up-to-date and continuously running, traditional signature-based AV will protect an endpoint from infection by most known malware families. The problem is that they are simply unable to detect and block novel or altered versions – such as if the malware has been repacked – until a human manually writes a new detection signature is created and pushed out to the endpoints in the form of an update.

AV is also extremely resource heavy – not just to produce new signatures and keep devices up to date, it also requires a lot of resource consumption on the endpoint as new signatures are downloaded and the device is rescanned daily.

Scans are time consuming because they essentially have to look for every single piece of malware every single time. Realistically that is not possible, so they stop looking for older malware versions, attackers often resurrect them, and AV misses the detection. This is where NGAV comes into play.

NEXTGEN ANTIVIRUS (NGAV)

NGAV solutions usually employ Artificial Intelligence (AI) machine learning (ML) for detections based on the pre-execution characteristics of the code. This means they do a decent job of recognizing and blocking novel and altered malware strains that traditional AV misses and new detections are not constrained by the manual process of signature development.

NGAV has its limitations, often missing some unique malware variants and producing a high volume of false positives. The inability to prevent 100% of malware – in addition to the introduction of living-off-the-land, fileless, and other advanced attack techniques – prompted the advent of Endpoint Detection and Response (EDR) and its more comprehensive cousin Extended Detection and Response (XDR).

ENDPOINT DETECTION AND RESPONSE (EDR)

EDR delivered the ability to leverage AI/ML algorithms to analyze behaviors on the network to identify malicious operations in progress. It also enabled security teams to proactively threat hunt in their environments for the more subtle indicators of compromise that can expose an attack at subsequent stages.

EDR changed the entire security landscape for the better, but it also has its limitations. First, the AI/ML models are tremendously complex and take years to train, and the detections are only as good as the samples they were trained on. Also, EDR only provides acute visibility into what is happening on the endpoint, with limited visibility of the other network components aside from how they interact with those devices.

Employees are often the first line of defense against ransomware attacks.

EXTENDED DETECTION AND RESPONSE (XDR)

XDR solutions on the other hand, were designed as a logical extension of EDR with the benefit of correlating behavioral telemetry from other parts of the network. In this way, security teams can see not just what is happening on the endpoint, but also how that behavior is possibly related to user identity and authentication, or assets in the cloud, and across the entire IT and security stack.

XDR, while promising, still suffers from the same issues as other EPP tools: they are susceptible to bypassing and unhooking, they are difficult to configure and manage properly, and they usually have a high false positive rate – all of which means additional strain on already maxed-out security teams.

They also are dependent on complex AI/ML behavior detection models that take years to create, so they are not very agile when it comes to updating them as threat actor TTPs evolve. It is a tremendous lift to introduce a new model into production in client environments, and a small flaw in the training data for the model can mean big problems for its efficacy.

EMPLOYEE AWARENESS TRAINING

Employees are often the first line of defense against ransomware attacks. Human errors, such as clicking on malicious links or opening infected email attachments, can inadvertently invite ransomware into your organization. CXOs should prioritize ongoing employee cybersecurity training and awareness programs to reduce these risks.

Creating a cybersecurity-aware culture can empower employees to recognize and report potential threats, bolstering the organization's overall security posture. Yes, employees need to exercise a reasonable level of discretion in their daily work to ensure they are not providing an easy avenue for attackers; that said, as an industry we need to abandon the "weakest link" excuse for the failure of our security operations up and down the stack.

Yes, employees are going to click on malicious links and open tainted attachments. Why? Because they are busy and distracted doing their jobs. And just as security staff are not overly involved with things like marketing budgets, customer acquisition and retention campaigns, facilities management and other critical business operations, corporate staff should not be expected to be the front lines for network defense.

In the case of a ransomware attack that starts with a phishing expedition, sure, maybe the employee messed up by clicking a bad link in a moment of distraction. We can all pile on them for not noticing the spelling error or poor grammar in the email, or that the URL was a typo-squat, or that the email metadata did not match up with the contents of the email, etc.

But where did security really fail? It failed when it did not block the malicious email for the same reasons, we want to blame the errant employee. It failed when it allowed malicious code to execute on the network. It failed when it allowed command and control to be established and additional executables to be downloaded. It failed when lateral movement and credential theft was not detected. It failed when it did not block sequences leveraging native network tools when the behavior was outwardly malicious. It failed when it did not detect and block the data exfiltration. And it failed when it did not prevent critical data and systems from being encrypted.

When you evaluate an attack like this and consider all failures, blaming the failure of the security stack on one employee who mistakenly clicked a link is ridiculous. Millions of dollars of security that can be undone by one click is the problem, not the person who clicked.

02 CXO-Specific Roles and Responsibilities

CEO: CHIEF EXECUTIVE OFFICERS

By fostering a culture of security, Chief Executive Officers can create an environment where employees understand the importance of protecting the organization's digital assets and are actively engaged in preventing ransomware attacks. Here are several items a CEO should take to address company culture regarding ransomware threats:

Leadership commitment

The CEO should demonstrate a strong commitment to cybersecurity by actively engaging in the development and implementation of security strategies, allocating appropriate resources, and emphasizing its importance during company-wide communications. Support for a security first culture and program is key to establishing a direction within the organization. This top-down approach will signal to employees that cybersecurity is a priority for the organization.

Education and training

Implement regular security training programs for all employees, regardless of their role in the company. This training should include information on ransomware threats, how they can infiltrate an organization, and the potential consequences of an attack. Additionally, provide employees with guidelines and best practices for identifying and avoiding phishing emails, safely handling sensitive information, and reporting any suspicious activity.

Open communication

Encourage open communication between employees and the security team. Establish clear channels for employees to report potential security concerns and ensure that they feel comfortable doing so without fear of negative consequences. This open dialogue can help identify and address vulnerabilities before they are exploited by cybercriminals.

Incentivizing secure behavior

Recognize and reward employees who exhibit secure behavior, contribute to the organization's cybersecurity efforts, or report potential security issues. This can create a positive reinforcement loop that encourages others to adopt secure practices.

Regular evaluation and improvement

Continuously assess the effectiveness of your organization's cybersecurity culture and adjust your strategies as needed. Solicit feedback from employees on the training programs, communication channels, and security policies to identify areas for improvement.

Collaboration across departments

Foster a sense of shared responsibility for cybersecurity by promoting collaboration between IT, security, and other departments. By integrating security into the daily operations of all teams, employees will better understand the role they play in safeguarding the organization from ransomware threats.

Incident response preparedness

Ensure that employees are aware of the organization's incident response plan and understand their roles in the event of a ransomware attack. Regularly test and update the plan to maintain its effectiveness and ensure a coordinated response to any potential threats.

CEO: CHIEF EXECUTIVE OFFICERS

By fostering a culture of security, Chief Executive Officers can create an environment where employees understand the importance of protecting the organization's digital assets and are actively engaged in preventing ransomware attacks. Here are several items a CEO should take to address company culture regarding ransomware threats:

Leadership commitment: The CEO should demonstrate a strong commitment to cybersecurity by actively engaging in the development and implementation of security strategies, allocating appropriate resources, and emphasizing its importance during company-wide communications. Support for a security first culture and program is key to establishing a direction within the organization. This top-down approach will signal to employees that cybersecurity is a priority for the organization.

Education and training: Implement regular security training programs for all employees, regardless of their role in the company. This training should include information on ransomware threats, how they can infiltrate an organization, and the potential consequences of an attack. Additionally, provide employees with guidelines and best practices for identifying and avoiding phishing emails, safely handling sensitive information, and reporting any suspicious activity.

Open communication: Encourage open communication between employees and the security team. Establish clear channels for employees to report potential security concerns and ensure that they feel comfortable doing so without fear of negative consequences. This open dialogue can help identify and address vulnerabilities before they are exploited by cybercriminals.

Incentivizing secure behavior: Recognize and reward employees who exhibit secure behavior, contribute to the organization's cybersecurity efforts, or report potential security issues. This can create a positive reinforcement loop that encourages others to adopt secure practices.

Regular evaluation and improvement: Continuously assess the effectiveness of your organization's cybersecurity culture and adjust your strategies as needed. Solicit feedback from employees on the training programs, communication channels, and security policies to identify areas for improvement.

Collaboration across departments: Foster a sense of shared responsibility for cybersecurity by promoting collaboration between IT, security, and other departments. By integrating security into the daily operations of all teams, employees will better understand the role they play in safeguarding the organization from ransomware threats.

Incident response preparedness: Ensure that employees are aware of the organization's incident response plan and understand their roles in the event of a ransomware attack. Regularly test and update the plan to maintain its effectiveness and ensure a coordinated response to any potential threats.

CFO: CHIEF FINANCIAL OFFICERS

A Chief Financial Officer's role in addressing company culture as it relates to ransomware threats is vital, as they must ensure that financial resources are allocated appropriately to support cybersecurity initiatives while fostering a culture of risk awareness and fiscal responsibility. Here are several ways a CFO can address company culture in the context of ransomware threats:

Align cybersecurity investments with business objectives: A CFO should ensure that cybersecurity investments are aligned with the organization's overall business objectives and risk appetite. This involves working closely with other C-level executives, IT, and security teams to identify, prioritize, and allocate resources to the most critical cybersecurity initiatives, including those focused on ransomware prevention and mitigation.

Promote a risk-aware culture: A CFO should actively promote a risk-aware culture throughout the organization. This involves educating employees about the financial consequences of ransomware attacks, including the costs associated with downtime, data loss, and reputational damage. By helping employees understand the potential fiscal impact of ransomware attacks, they will be more likely to take cybersecurity seriously and adopt secure practices in their day-to-day work.

Evaluate the need for cyber insurance: A CFO should assess the organization's need for cyber insurance, considering the potential costs associated with ransomware attacks and the organization's risk tolerance. Cyber insurance can provide additional financial protection and help the organization recover more quickly from a ransomware attack. By evaluating and, if necessary, investing in cyber insurance, a CFO demonstrates a commitment to managing the financial risks associated with ransomware.

Monitor the effectiveness of cybersecurity investments: A CFO should regularly monitor and assess the effectiveness of cybersecurity investments, including those aimed at preventing and mitigating ransomware attacks. This can involve developing and tracking key performance indicators (KPIs) related to cybersecurity and adjusting investments as needed to maximize their impact.

Collaborate with other C-level executives: A CFO should collaborate closely with other C-level executives, including the CEO, CIO, and CISO, to ensure a coordinated approach to addressing ransomware threats. By working together, these executives can develop comprehensive strategies that balance financial resources, risk management, and operational efficiency.

Support employee training and awareness initiatives: A CFO should support and allocate resources for employee training and awareness initiatives related to ransomware threats. By investing in training, a CFO helps to create a culture where employees understand their role in preventing ransomware attacks and are equipped with the knowledge and skills to do so effectively.

A CFO should actively promote a risk-aware culture throughout the organization.

CIO: CHIEF INFORMATION OFFICERS

A Chief Information Officer's role in addressing company culture as it relates to ransomware threats is essential, as they are responsible for implementing technology solutions and processes to protect the organization's digital assets. Here are several ways a CIO can address company culture in the context of ransomware threats:

Promote a security-first mindset: A CIO should actively promote a security-first mindset throughout the organization. This involves emphasizing the importance of cybersecurity in all aspects of the business, from IT infrastructure and software development to employee training and communication. By prioritizing security, employees will be more likely to adopt secure practices and take their role in preventing ransomware attacks seriously.

Implement robust security measures: A CIO should ensure that robust security measures are in place to protect the organization from ransomware threats. This includes implementing advanced threat detection and prevention tools, enforcing strong access controls, and maintaining a rigorous patch management system to minimize vulnerabilities that can be exploited by cybercriminals.

Support employee training and awareness initiatives: A CIO should allocate resources and support employee training and awareness initiatives related to ransomware threats. This involves providing employees with guidelines and best practices for identifying and avoiding phishing emails, safely handling sensitive information, and reporting any suspicious activity. Regular training and awareness programs can help employees recognize and respond to ransomware threats more effectively.

CISO: CHIEF INFORMATION SECURITY OFFICERS

A Chief Information Security Officer's role in addressing company culture as it relates to ransomware threats is critical, as they are responsible for designing and implementing the organization's cybersecurity strategy and ensuring that employees understand the importance of protecting digital assets. Here are several ways a CISO can address company culture in the context of ransomware threats:

Develop a comprehensive cybersecurity strategy: A CISO should develop and implement a comprehensive cybersecurity strategy that addresses ransomware threats, along with other potential cyber risks. This strategy should be aligned with the organization's business objectives, risk appetite, and available resources, and should be regularly reviewed and updated to account for evolving threats and technologies.

Establish a risk-based cybersecurity framework: A CISO should establish a risk-based cybersecurity framework that identifies, assesses, and prioritizes the organization's risks related to ransomware and other cyber threats. This

framework should be aligned with the organization's business objectives, risk tolerance, and available resources, and should be regularly reviewed and updated to account for evolving threats and technologies.

Promote a culture of shared responsibility: A CISO should actively promote a culture of shared responsibility for cybersecurity throughout the organization. This involves emphasizing the importance of each employee's role in preventing ransomware attacks and encouraging cross-departmental collaboration on cybersecurity initiatives. By fostering a sense of collective ownership, employees will be more likely to adopt secure practices and take their role in preventing ransomware attacks seriously.

Develop and implement security policies and procedures: A CISO should develop and implement security policies and procedures that address ransomware threats, along with other potential cyber risks. These policies should be clearly communicated to all employees and should be regularly reviewed and updated to ensure they remain effective toward evolving threats.

Support employee training and awareness initiatives: A CISO should allocate resources and support employee training and awareness initiatives related to ransomware threats. This involves providing employees with guidelines and best practices for identifying and avoiding phishing emails, safely handling sensitive information, and reporting any suspicious activity. Regular training and awareness programs can help employees recognize and respond to ransomware threats more effectively.

Collaborate with other C-level executives: A CISO should collaborate closely with other C-level executives, including the CEO, CFO, and CIO, to ensure a coordinated approach to addressing ransomware threats. By working together, these executives can develop comprehensive strategies that balance technological solutions, risk management, and financial resources.

Plan and Run Tabletop Exercises: A CISO should plan out and run periodic tabletop exercises that examine realistic scenarios the business might face. These exercises should involve all relevant C-level executives and external parties that may need to be involved such as outside counsel, crisis management/comms, etc. It is helpful to have work through the thresholds of when and if payments should be considered.

Develop and maintain an incident response plan: A CISO should lead the development of a comprehensive incident response plan that specifically addresses ransomware attacks. This plan should outline the roles and responsibilities of various stakeholders, establish clear communication channels and escalation paths, and detail the steps to be taken in the event of an attack. Regular testing and updating of the incident response plan are essential to ensure its effectiveness in a real-world scenario.

COO: CHIEF OPERATING OFFICERS

A Chief Operating Officer's role in addressing company culture as it relates to ransomware threats is crucial, as they are responsible for ensuring that the organization's operations can continue smoothly in the face of potential cyberattacks. Here are several ways a COO can address company culture in the context of ransomware threats:

Develop a business continuity plan

A COO should develop and maintain a comprehensive business continuity plan which accounts for the potential impact of a ransomware attack on critical operations. This plan should include contingencies for short- and long-term disruptions and strategies for recovering from an attack and resuming normal operations as quickly as possible.

Promote a culture of operational resilience

A COO should actively promote a culture of operational resilience throughout the organization. This involves emphasizing the importance of maintaining business continuity in the face of potential cyberattacks and encouraging employees to be proactive in identifying and addressing potential vulnerabilities in the organization's processes and systems.

Assess third-party vendor risks

A COO should assess the risks associated with third-party vendors and service providers, as these relationships can potentially introduce ransomware threats to the organization. By implementing robust vendor management processes and ensuring that vendors adhere to the organization's cybersecurity requirements, a COO can help minimize the likelihood of a ransomware attack originating from a third party.

Collaborate with other executives

A COO should collaborate closely with other C-level executives, including the CEO, CFO, CIO, and CISO, to ensure a coordinated approach to addressing ransomware threats. By working together, these executives can develop comprehensive strategies that balance operational resilience, risk management, and financial resources.

Support employee training and awareness initiatives

A COO should allocate resources and support employee training and awareness initiatives related to ransomware threats. By investing in training, a COO helps to create a culture where employees understand their role in maintaining business continuity and are equipped with the knowledge and skills to effectively respond to ransomware attacks.

Regularly review and update operational processes

A COO should regularly review and update operational processes to ensure they remain resilient in the face of evolving ransomware threats. This may involve implementing additional security measures, adjusting workflows to minimize the potential impact of a ransomware attack, or adopting new technologies to improve the organization's overall operational resilience.

CPOS: A CHIEF PRIVACY OFFICER

CPOs: A Chief Privacy Officer's role in addressing company culture as it relates to ransomware threats is significant, as they are responsible for ensuring the protection and privacy of the organization's sensitive data. Here are several ways a CPO can address company culture in the context of ransomware threats:

Develop and enforce data privacy policies: A CPO should develop and enforce data privacy policies that address the potential risks associated with ransomware attacks. These policies should outline the proper handling, storage, and disposal of sensitive data, as well as the steps to be taken in the event of a data breach resulting from a ransomware attack. Regularly reviewing and updating these policies is essential to ensure they remain effective and compliant with evolving privacy regulations.

Promote a culture of data privacy awareness: A CPO should actively promote a culture of data privacy awareness throughout the organization. This involves emphasizing the importance of protecting sensitive data from unauthorized access, both in the context of ransomware attacks and more broadly. By prioritizing data privacy, employees will be more likely to adopt secure practices and take their role in preventing data breaches seriously.

Support employee training and awareness initiatives: A CPO should allocate resources and support employee training and awareness initiatives related to ransomware threats and data privacy best practices. This involves providing employees with guidelines and best practices for handling sensitive data, identifying and avoiding phishing emails, and reporting any suspicious activity. Regular training and awareness programs can help employees recognize and respond to ransomware threats and data breaches more effectively.

Collaborate with other C-level executives: A CPO should collaborate closely with other C-level executives, including the CEO, CFO, CIO, and CISO, to ensure a coordinated approach to addressing ransomware threats and data privacy concerns. By working together, these executives can develop comprehensive strategies that balance data protection, risk management, and operational efficiency.

A CPO should regularly monitor the organization's compliance with data privacy regulations.

Monitor compliance with data privacy regulations: A CPO should regularly monitor the organization's compliance with data privacy regulations, such as the GDPR or CCPA, and address any gaps or weaknesses that could increase the risk of a data breach resulting from a ransomware attack. This may involve updating internal processes, implementing new technologies, or working with legal and compliance teams to ensure the organization remains compliant with applicable privacy laws.

Establish an incident response plan for data breaches: A CPO should lead the development of an incident response plan that specifically addresses data breaches resulting from ransomware attacks. This plan should outline the roles and responsibilities of various stakeholders, establish clear communication channels and escalation paths, and detail the steps to be taken in the event of a breach. Regular testing and updating of the incident response plan are essential to ensure its effectiveness in a real-world scenario.

CSO: CHIEF SECURITY OFFICER

A Chief Security Officer's role in addressing company culture as it relates to ransomware threats is vital, as they are responsible for overseeing the organization's overall security posture and ensuring that employees are aware of and prepared for potential cyber threats. Here are several ways a CSO can address company culture in the context of ransomware threats:

Develop a comprehensive security strategy: A CSO should develop and implement a comprehensive security strategy that addresses ransomware threats, along with other potential cyber risks. This strategy should be aligned with the organization's business objectives, risk appetite, and available resources, and should be regularly reviewed and updated to account for evolving threats and technologies.

Promote a security-first mindset: A CSO should actively promote a security-first mindset throughout the organization. This involves emphasizing the importance of security in all aspects of the business, from IT infrastructure and software development to employee training and communication. By prioritizing security, employees will be more likely to adopt secure practices and take their role in preventing ransomware attacks seriously.

Implement robust security measures: A CSO should ensure that robust security measures are in place to protect the organization from ransomware threats. This includes implementing advanced threat detection and prevention tools, enforcing strong access controls, and maintaining a rigorous patch management system to minimize vulnerabilities that can be exploited by cybercriminals.

Support employee training and awareness initiatives: A CSO should allocate resources and support employee training and awareness initiatives related to ransomware threats. This involves providing employees with guidelines and best practices for identifying and avoiding phishing emails, safely handling sensitive information, and reporting any suspicious activity. Regular training and awareness programs can help employees recognize and respond to ransomware threats more effectively.

Collaborate with other C-level executives: A CSO should collaborate closely with other C-level executives, including the CEO, CFO, CIO, and CISO, to ensure a coordinated approach to addressing ransomware threats. By working together, these executives can develop comprehensive strategies that balance technological solutions, risk management, and financial resources.

Foster a culture of continuous improvement: A CSO should foster a culture of continuous improvement in the organization's security posture. This involves regularly assessing and updating security measures, processes, and policies to ensure they remain effective in the face of evolving ransomware threats. By encouraging employees to stay up to date with the latest security best practices, a CSO can help create an environment where employees are proactive in preventing and responding to ransomware attacks.

Takeaway

Ransomware attacks pose a significant threat to organizations of all sizes and industries. C-level executives must take a proactive and collaborative approach to understanding and mitigating the risks associated with ransomware. By fostering a culture of cybersecurity, investing in the right technologies and personnel, and developing comprehensive incident response and business continuity plans, organizations can minimize the impact of ransomware attacks and maintain a strong security posture.

By understanding and addressing the unique challenges that ransomware presents, C-level executives can work together to protect their organizations and maintain the trust of their customers and employees. Ransomware attacks pose a significant and evolving threat to businesses of all sizes and industries. CXOs must be proactive in understanding the potential impact of these attacks and the risks they pose to the organization. Financial costs, operational disruption, data loss, reputational damage, legal consequences, and the evolving threat landscape are all factors that demand attention.

To protect your business, invest in robust cybersecurity measures, engage in ongoing employee training, and cultivate a culture of cybersecurity awareness. Collaborate with legal counsel to navigate the legal and regulatory landscape and develop a crisis communication plan to address reputational damage.

By taking these steps, CXOs can reduce the risk of ransomware attacks and ensure the long-term resilience of their organizations in the face of this evolving threat.

The Halcyon Mission: Defeat Ransomware

Legacy security tools were simply not designed to address the unique threat that ransomware presents, so we keep seeing destructive ransomware attacks circumvent these solutions.

The Halcyon Anti-Ransomware Platform:

- Detects and blocks both known and novel ransomware families via multi-layer, AI-powered prevention, detection and response engines.
- Delivers built-in endpoint agent hardening and ensures existing solutions are protected from bypass and unhooking techniques.
- Provides redundant resiliency features through autonomous host isolation and encryption key capture for swift automated recovery.

The unique Halcyon Anti-Ransomware Platform is easy to deploy, does not conflict with existing endpoint security solutions, and provides multiple, unique levels of protection against ransomware attacks. Halcyon is the first platform to leverage advanced AI/ML detection models specifically trained to defeat ransomware.

Talk to a Halcyon expert today to find out more and check out our Recent Ransomware Attacks resource site to get near real-time tracking of ransomware attacks, threat actor groups and their victims.

halcyon