A Research Study on the

2021 State of **RANSOMWARE** Preparedness

axio®

Executive Summary

Axio's research study on the 2021 State of Ransomware Preparedness reveals several concerning findings about the general state of organizational readiness to combat the growing tide of ransomware.

Overall, most organizations surveyed are not adequately prepared to manage the risk associated with a ransomware attack, and many organizations continue to lack the basic cybersecurity controls required to defend against ransomware. Axio identified 7 key areas where organizations are deficient in implementing and sustaining basic cybersecurity practices.

Key Findings

- **Failing to implement and maintain fundamental cybersecurity practices** and cyber hygiene is over-exposing organizations to ransomware.

- **Highly impactful improvements in ransomware protection** can be made through a back-to-basics approach.

- **Deficiencies in identity and access management are pervasive.** In particular, a lack of focus on foundational practices and tools for managing privileged access is widespread and may be the leading contributor to poor organizational resistance to ransomware.

- **Recommitting to fundamental cybersecurity practices** and controls may fortify ransomware defenses with low investment and implementation barriers

Key Datapoints

- Nearly 80% of organizations responded that they have not implemented or have only partially implemented a privileged access management solution.

- Only 36% of respondents indicated that they audit the use of service accounts, a type of privileged account, on a regular basis.

- Only 26% of respondents deny the use of command-line scripting tools (such as PowerShell) by default.

- 69% of organizations indicated that they do not limit access to the internet for their Windows domain controller hosts.

- Only 29% of respondents evaluate the cybersecurity posture of external parties prior to allowing them access to the organization's network.

- Only 50% of respondents conduct user awareness training for employees on email and web-based threats, such as spear-phishing and watering hole attacks, on an annual basis.

Introduction

The headlines tell the story of our times: ransomware is everywhere. It dominates the news cycles and it's on the agenda for many corporate board meetings. It is one of the cornerstones of the Biden administration's effort to classify ransomware as a national security threat [1]. And for good reason. High-visibility, high-impact ransomware attacks continue to do untold damage on many of the Nation's critical infrastructure sectors. After the much-publicized SolarWinds attack—which raised our collective consciousness to the use of routine software updates to deliver ransomware—we are continuing to see a variety of attacks and coining a new reality: ransomware-as-a-service [2]. And many of these attacks are focused on critical infrastructure where they can cause the most disruption and economic damage.

Most recently, Iowa-based provider of agriculture services NEW Cooperative, Inc was the victim of a ransomware attack by BlackMatter, forcing them to take their systems offline and disrupting the public supply of grain, pork, and chicken [3]. Interestingly, a recently-published article claimed that in a private conversation with the attacker, NEW Cooperative representatives complained that BlackMatter has asserted on their website that they do not attack critical infrastructure [4]. Lesson learned: ransomware attackers get to make the rules and break them as they see fit.

Early ransomware attacks were primarily focused on holding an organization's data hostage. But, as companies have gotten better at data backup and recovery, ransomware attacks have evolved to taking over systems and networks, setting up command and control operations, and stealing data and intellectual property. This shift in tactics and objectives is especially troublesome for critical infrastructure operators who are tasked with providing some of society's most vital and life-sustaining services. Because of the interconnected nature of critical infrastructure, damage that is not immediately contained locally can spread quickly across an entire sector.

Evolving to an Internet-focused and networked technical environment is certainly expanding the threat environment for ransomware. But, is this the primary reason why organizations are finding it more difficult to defend against the threat? Is it a simple case that organizations have not adjusted or evolved their cybersecurity strategies, practices, and controls to the new operating environment? Or, in the rush to embrace the latest technology, have they simply lost focus on the basics?

Research Methodology

The Axio360 platform provides users a unique opportunity to evaluate their readiness to address ransomware priorities through the Ransomware Preparedness assessment. This new assessment tool is based on data from hundreds of real ransomware events, guidance from the U.S. Department of Homeland Security, and Axio's own research.

To date, more than 100 organizations across multiple critical infrastructure sectors have used the tool to determine their cybersecurity posture against ransomware. Using the assessment, organizations are asked to rate the degree to which a specific practice is implemented—from Fully Implemented to Largely, Partially, and Not Implemented. The practices are curated from domains such as Vulnerability Management, Privileged Access Management, Network Monitoring, and Incident Management.

Using de-identified data collected from organizations that have completed the Ransomware Preparedness assessment, Axio researchers set out to identify potential patterns and emergent properties that might provide insight into why organizations may be increasingly susceptible to ransomware attacks.

The value of this data—as opposed to direct surveying—is that organizations who participate in the assessment are motivated to identify program gaps and address them to improve their overall resilience to ransomware.

Because the assessment includes essential cybersecurity practices, participants can re-examine them in a ransomware context and determine if the practice needs to be expanded, tweaked, or built-back-better. This allows participants to refocus on an expanding threat landscape—one that is increasingly dominated by some form of ransomware.

A Key Observation

The consensus of many recent articles and papers on ransomware exposure and preparedness have established that the rise in ransomware is due to several factors that may not be in the direct control of the organization. For example, the lack of sufficient technologies to defend against or prevent ransomware attacks is a common justification for why organizations have fallen behind. Additionally, the rapidly increasing number of attacks is frequently cited as a barrier to effective ransomware management, as is the propensity of employees to fall victim to phishing schemes and use poor judgment when using the Internet.

> **While these are undeniable truths that organizations must confront, there is still a lot of defensive power in the organization that can be harnessed to bolster resilience to ransomware attacks.**

Thus, we examined our data with an eye toward identifying factors that are more typically in the organization's direct control—that can be improved without significant barriers or in some cases, additional investment. And, an interesting observation emerged: organizations may have taken their eye off of sustaining the most fundamental cybersecurity practices. They are failing at the basics. While this may not completely explain why organizations are increasingly falling victim to ransomware attacks, it is undeniably a contributing factor.

What We Found

As we suspected, our data identified 7 key areas where organizations are deficient in implementing and sustaining basic cybersecurity practices. This is important because it indicates that some of the improvement in ransomware defense may be directly attainable by re-committing to improving basic cyber hygiene.

The term “hygiene” encompasses the basic activities that focus on maintaining health and preventing undesirable outcomes—disease, disruption, or failure. Applied to the cyber world, hygiene implies a focus on the fundamental controls and practices that ensure the security and operational resiliency of an organization’s critical assets, such as systems, infrastructure, and data. Cleanliness is at the heart of cyber hygiene. Practically speaking, this means that asset configurations are free of vulnerabilities, have unnecessary and insecure services and communication ports shut down, allow only limited access to the Internet or other unnecessary network segments, constrain administrative access to a limited number of privileged users, and are subjected to frequent “health” monitoring for anomalies and performance. As with personal hygiene, it’s a game of prevent now or pay later: committing to basic hygiene at implementation can ward off costly and destructive damage down the road. With this in mind, we set out to determine if the success of ransomware attacks might be related on some level to obvious deficiencies in fundamental practices.

The following represents the core findings of our examination of assessment data. For background, we analyzed responses to 65 core practices in 8 domains. We identified the practices where a majority of the respondents indicated that the practice was either Not implemented or only Partially implemented (with the assumption that the practice was incomplete or not operational.) The practices were then analyzed and grouped to identify emergent themes as discussed in this section.

Management of Privileged Access

Overwhelmingly, the most concerning finding in our data was the pervasive lack of basic controls over privileged credentials and access.

According to Gartner, privileged access management is defined as foundational security technology to protect accounts, credentials and operations that offer an elevated or “privileged” level of access [5]. At a program level, privileged access management encompasses controls, practices, and supporting technologies that facilitate the administrative needs of privileged users in balance with reasonable limitations on excessive, inappropriate, and ultimately, insecure use. From a functional perspective, privileged access management comprises a range of capabilities such as providing a secure vault for storing credentials, recording the use of credentials through session management and keystroke monitoring, and providing a platform for forensic auditing of credential use, which can be especially important in incident management. Additionally, done well, a privileged access management capability will provide additional layers of protection by obfuscating credentials while vaulted—in essence, protecting the credential so that even privileged users cannot "steal it" or otherwise abuse it. Because privileged credentials are the most powerful keys to the organization's infrastructure, the importance of keeping them secure, in the right hands, and with appropriate use limitations is paramount to a strong ransomware attack defense. In fact, poor credential management may be the single biggest contributor to the success of ransomware breaches and the extent of damage caused.

Ransomware attackers often prioritize "training-run" attacks to gain access to privileged credentials so that they can be used to develop full-blown, more extensive, and more destructive ransomware campaigns. The use of privileged credentials for ransomware attacks typically results in much more extensive and widespread control over an organization's network and computing assets, making it much more difficult to eradicate. In essence, a more involved ransomware attack increases the attacker's chances of getting their victim to relent and pay an extreme ransom.

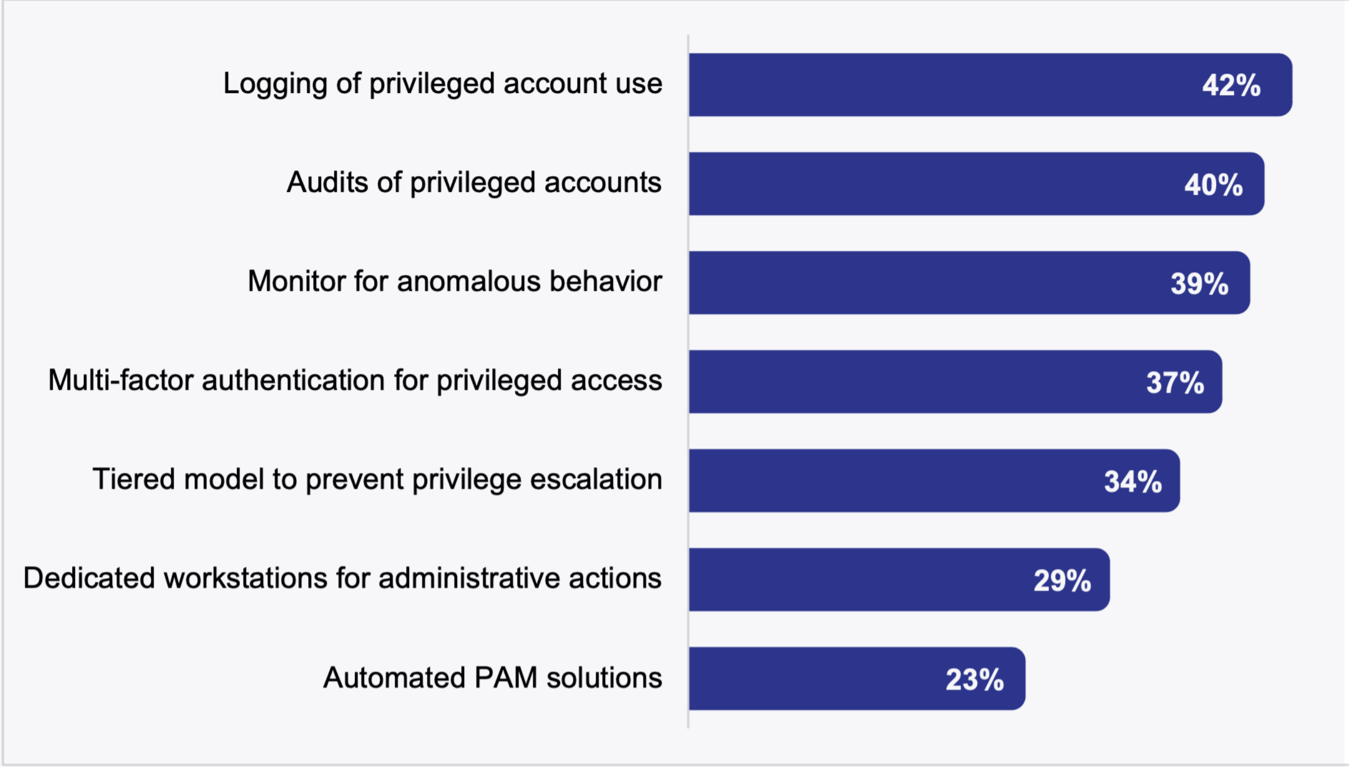
Our data indicates four key areas where fewer than 50% of respondents have implemented sufficient controls and practices to improve their management of privileged credentials:

- A clear failure to implement tool-based solutions to control access to and tracking of privileged credentials. Nearly 80% of organizations responded that they have not implemented or have only partially implemented a privileged access management tool.

- On a related note, the use of compensating controls for privileged access management does not appear to be in place. Fully 70% of respondents noted that they do not put restrictions on where privileged credentials can be used (i.e., they permit use on infrastructure that is not intended for administrative work), 63% have not fully or largely implemented two-factor authentication for using privileged credentials, and only 42% of respondents indicate that they log the activities performed with privileged credentials. Not only do respondents appear to be failing to log privileged activities, only a small minority of respondents (39%) indicated that they monitor for anomalous use of privileged credentials.

- Secure management of service accounts—a type of privileged account that is broadly used to execute infrastructure services, typically without human intervention—does not fair considerably better in our data. Because service accounts have vast capabilities that are essential to operating systems and infrastructure, these non-human accounts can be very dangerous if exposed or captured. And, because organizations often allow inappropriate use of these accounts by privileged users to manage infrastructure and perform administrative duties, they are more susceptible to capture because of mishandling and poor protection. This underscores the need to regularly audit the use of these accounts and correct out-of-bounds, unintended use. Unfortunately, only 36% of respondents indicated that they audit the use of service accounts on a regular basis and 38% review the access and privileges granted to service accounts on a regular basis.

Figure 1. Privileged Access Management
Practices Implemented by % of Respondents



Basic Cyber Hygiene

Cyber hygiene can have many definitions, but in simple terms, it refers to the implementation of basic practices and controls to protect the “health” of an organization’s network, assets, and data. Much cyber hygiene is preventative in that fundamental controls are designed into assets as they are deployed. For example, blocking access to the Internet for every server build reduces exposure to Internet-borne viruses and ransomware. And a major benefit of good cyber hygiene is that it is a typically low-investment activity (particularly if performed at the time of infrastructure build and implementation) with high potential payoff.

In our data, we observed several practices that indicate continuing poor cyber hygiene. For example:

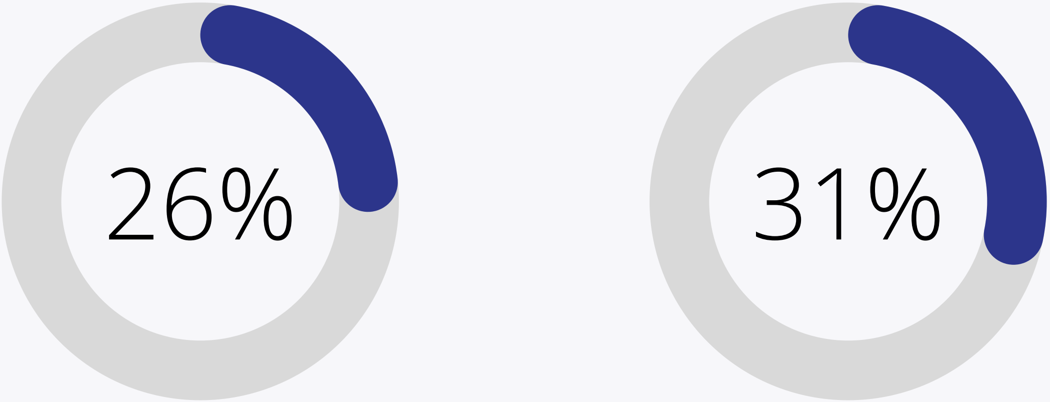
- Only 26% of respondents deny the use of command-line scripting tools (such as PowerShell) by default. These are powerful tools that should be restricted to authorized-use only and rarely provisioned to general users. In fact, best practice dictates that access to command-line scripting tools should be provisioned to authorized users only at the moment required and for only the duration of the authorized task.

- Sixty-nine percent (69%) of organizations indicated that they do not limit access to the Internet for their Windows domain controller hosts. Domain controllers are a pot-of-gold for attackers because they can use them to spread an attack laterally across the organization.

- Users continue to have access to local administrator accounts without limitation. Most users do not need these powerful accounts to do their daily jobs (except for when they want to bypass IT), yet 56% of our respondents have not disabled them. Worse yet, only 45% deny the use of these accounts by services, for batch jobs, or for remote access.

- The use of third-party software appears to be unabated. Over 70% of organizations noted they do not have exceptions or allow-listing processes in place to limit the acquisition and implementation of third-party software. This can create a shadow technology environment that may be exposed to unknown and unmanaged threats.

Figure 2. Basic Cyber Hygiene
Practices Implemented by % of Respondents



We deny the use of command line scripting tools.

We disable access to the internet for all Windows domain controller hosts.

Exposure to Supply Chain Risk

A world that is increasingly shifting to cloud-based computing and everything-as-a-service expands the threat landscape for organizations. Not only do organizations rely on external parties to provide key services, they may also have opened their networks to these parties to facilitate operational efficiency and convenience. For organizations with high degrees of externally provided systems and services, the threat landscape that is under their direct control may be very small. This is especially concerning for critical infrastructure providers such as electricity and natural gas providers because their operations often seamlessly cross geographic and technical boundaries that they do not directly control. Thus, one organization that inherits risk from an external provider can replicate that risk across an entire sector.

Our data indicates that organizations likely continue to be over-exposed to potential inherited threats from external providers. For example, we noted:

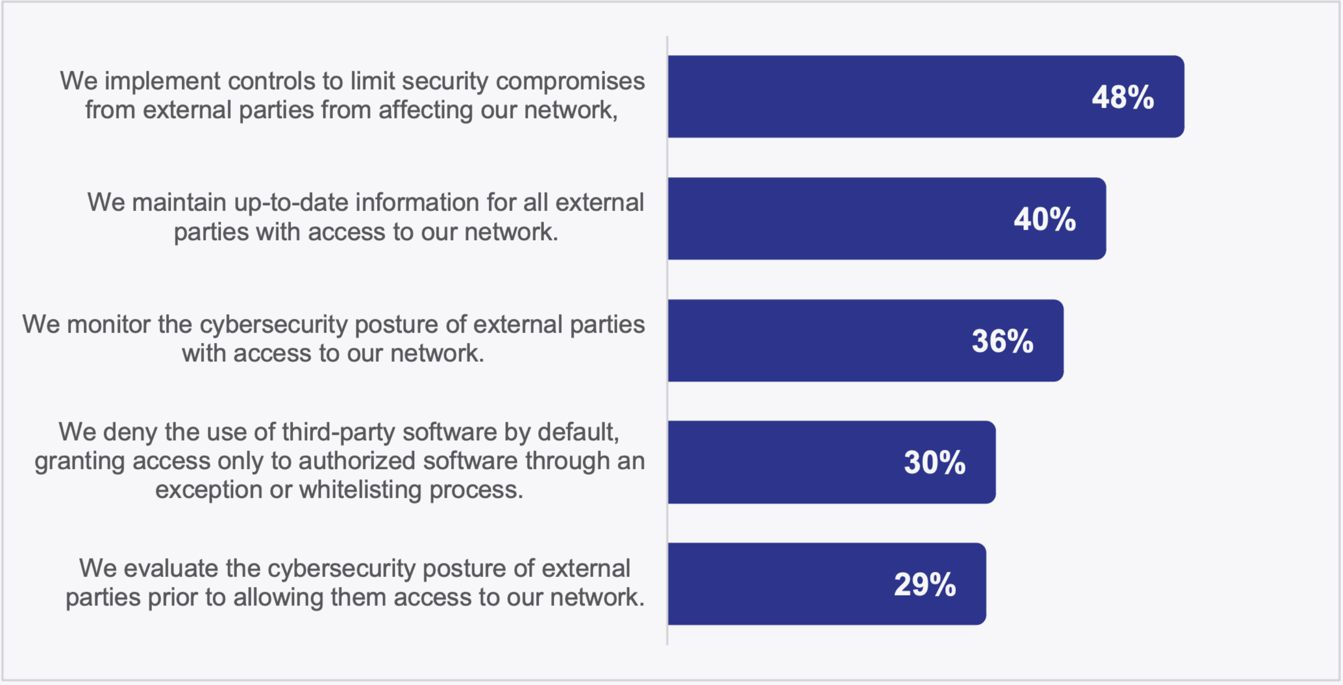
- Only 29% of respondents evaluate the cybersecurity posture of external parties prior to allowing them access to the organization's network. For these organizations, the degree to which they are exposed to potential ransomware attacks that may be delivered by external parties remains largely unknown.

- As a compounding concern, not only do organizations appear to be unaware of inherited risk, only 34% of respondents monitor the cybersecurity posture of external parties to whom they have provided direct network access. Additionally, 60% of respondents admit to not maintaining up-to-date information about the external parties that have access to their network. Combined, these deficiencies may manifest in unauthorized and undetected use of privileged credentials by external parties, particularly if there is a high degree of staff turnover in the external provider's organization.

- And, organizations do not appear to be implementing preventative controls to limit security compromises they may be exposed to through an external relationship. Only 48% of organizations relayed that they implement controls such as restricting account permissions or restricting network access to specific segments that can be monitored and controlled.

Figure 3. Exposure of Supply Chain Risk

Practices Implemented by % of Respondents



Network Monitoring

Network monitoring is unquestionably the front line of defense for proactively identifying and neutralizing ransomware attacks. Yet, our data indicates that many organizations may not have invested in basic network controls, nor do they monitor their networks for changes and anomalies that might indicate an intrusion. Just as an organization's network provides the backbone that connects users, communications, and systems, it is ironically also an excellent conduit for propagating malware and other malicious content.

Our data suggests organizations may be unnecessarily over-exposing their networks to ransomware intrusion.

- Basic network monitoring may not be in place. Sixty-eight percent (68%) of organizations do not monitor for deviations from an established baseline of network and system activity. In addition, a significant percentage of organizations do not monitor for and alert on anomalous connections to the network (55%) or for suspicious transfers of data and processes that use excessive network resources (64%).

- The use of basic segmentation controls may not be in place either. As a fundamental practice for limiting and containing potential damage, only 38% of respondents reported they segment their networks to block or control traffic to constrict lateral movement by malicious actors.

- Only 45% of respondents use controls to block uncategorized and newly registered domains using tools such as DNS or web proxy filters.

Incident Management

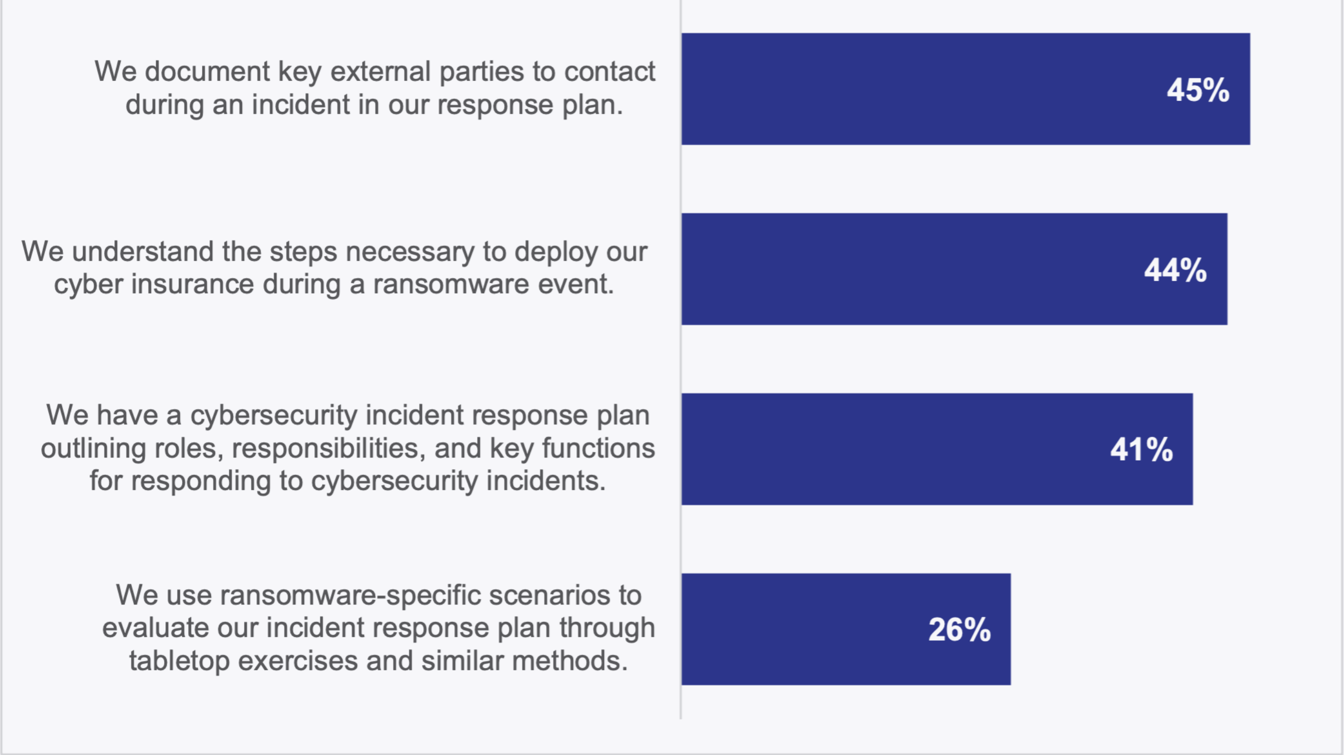
A focus on preventative controls and practices is certainly a primary investment in a layered defense-in-depth approach to addressing ransomware intrusions. However, as many high-profile attacks have reminded us, ransomware and other threats sometimes make their way into the organization and require decisive and timely action. Incident response plans now typically include a specific ransomware-focused playbook, particularly to ensure the threat is contained, spread is controlled, and organizational response is coordinated—with the intent to limit financial and reputational damage.

However, our data indicates that there is room for improvement when it comes to incorporating ransomware into incident management processes. And, it starts with having a fully developed and documented incident response plan. Unfortunately, only 41% of respondents had a plan that outlined roles, responsibilities, and key functions for responding to a cybersecurity incident, and of those who had a plan in place, only 21% included a ransomware-specific playbook in their plan. Additionally:

- A minority of respondents (45%) documented in their plan key external parties that would be relied upon to provide support services during an incident, such as IT systems management, forensics, legal guidance, law enforcement, and external public relations. These services may be difficult to procure in a timely manner without pre-existing relationships, contracts, and in some cases, financial retainers already in place.

- Additionally, for the organizations that have procured insurance protections in their response plan, only 44% documented the steps necessary to obtain coverage during a ransomware event. This is important because insurance providers may have very specific, sequential actions that must be taken to preserve coverage during an incident.

Figure 4. Incident Management
Practices Implemented by % of Respondents



Vulnerability Management

Intelligence about exploitable vulnerabilities is another essential tool in the prevention of ransomware intrusions, but only where known vulnerabilities—especially critical ones—are remediated on a timely basis. The time-to-remediate can be a critical metric that indicates the length of exposure to a potential ransomware threat. Longer times-to-remediate equal increased (and unnecessary) exposure to ransomware risk, giving attackers more time to perfect their approach and exploit organizations that have not acted to remediate. In fact, according to the National Security Agency, hackers breached the credit agency Equifax using a publicly-known vulnerability a mere 24 hours after details were made public in March 2017 [6]. This indicates that hackers are weaponizing vulnerability information at an alarmingly-efficient rate.

As an essential cornerstone of cybersecurity practice, vulnerability management remains one of the more difficult activities to do well, requiring not only a large labor investment, but a highly coordinated orchestration across IT departments and business users. Done poorly, remediation can cause operational interruptions and worse yet, extended disruptions that can require walk-back actions.

Our data confirms that organizations continue to struggle with vulnerability management overall. For example:

- A small majority (54%) scan all systems and applications in their network for vulnerabilities at least quarterly. Unfortunately, timely vulnerability identification is fundamental to understanding and managing exposure to ransomware, and given the volume of vulnerabilities in modern systems, applications, and infrastructure, even quarterly scanning can lead to unacceptable exposure and time-to-remediate.

- For respondents that perform vulnerability identification on a regular basis, only 32% percent require critical vulnerabilities to be patched within 24 hours, and further, achieve that requirement more than 95% of the time. Only 47% remediate all identified vulnerabilities that are known to have potential for compromise.

Training and Awareness

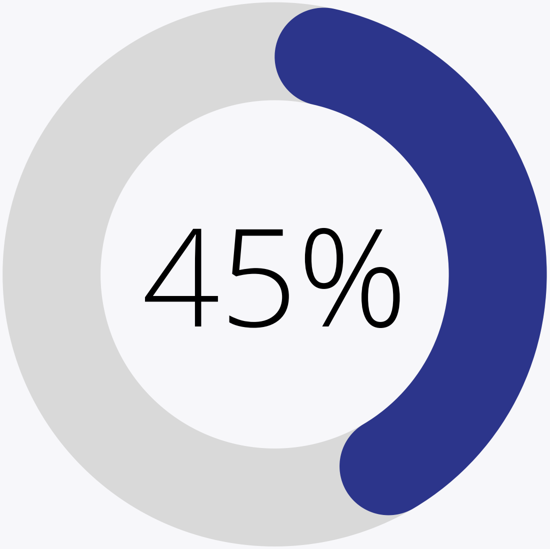
Anyone who is assigned user credentials in an organization—whether they are employees, contractors, or other external parties—are the first line of defense for ransomware attacks, particularly since they are the intended target of credential-harvesting phishing campaigns. Indeed, the well-publicized 2013 data breach of Target Corporation (which affected 41 million consumers and cost Target $18.5 million in restitution) is a classic example of obtaining user credentials from a third-party vendor through phishing, thereby allowing attackers access to Target's infrastructure where malware was installed. Consistent and pervasive training and awareness—for employees and non-employees—continues to be one of the best low-investment, high-payoff activities that an organization can use to prevent ransomware intrusion. Yet, while many organizations have made positive strides in this area, our data noted that there is still room for improvement.

- Only 50% of respondents conduct user awareness training for employees on email and web-based threats, such as spear-phishing and watering hole attacks, on an annual basis.

- More concerning, only 45% of organizations admit to conducting proactive phishing assessments to evaluate how well employees practice basic capabilities for identifying, reporting, and containing potential attacks.

Figure 5. Training and Awareness
Practices Implemented by % of Respondents

We conduct proactive phishing assessments to evaluate our employees' susceptibility to phishing attacks on at least a quarterly basis.



To be sure, the number and rate of increase of ransomware attacks is not slowing down. According to ThreatPost, there has been a significant increase in the level of ransomware attacks so far in 2021, up 151% for the first six months of the year compared to 2020. This translated to over 304 million attacks, outpacing the total number of attacks in 2020 [7]. Given this rapid increase in attacks, what conclusions can we draw relative to Axio's research findings?

While it is difficult to exactly correlate, it is not hard to imagine that a failure to implement basic cybersecurity practices and hygiene is a contributing factor to not only the increase in attacks, but the degree to which these attacks are successful. Ransomware attackers know from experience—their own research based on attacks they have already conducted—that organizations leave a lot of open doors. This is easily supported by how ransomware attackers are finding their way into an organization's infrastructure. According to Statista, the leading causes of ransomware infections in 2020 according to managed security providers (MSP) include phishing (54%), poor practices (27%), weak passwords and access management (21%), open RDP access (20%), and others. [8]. This is entirely consistent with Axio's assertion that

...organization's may be over-exposed as a result of their own failures to implement fundamental practices and controls.

Indeed, ransomware attackers are using more sophisticated attack vectors and rapidly increasing their attack surface. But, as evidenced in our research, the state of practice for addressing ransomware appears to be less-than-sufficient at the same time. These are concerning trends that will converge in more organizations being attacked, more attack attempts, and ultimately more damage. Unless organizations truthfully examine their basic practices and controls—as those who used the Axio360 Ransomware Preparedness tool did—the attacker's advantage will continue to grow.

In conclusion, the good news is that some of what needs to be fixed by organizations may not require significant investment or heavy lifting. A renewed focus on controlling and managing privileged access may be as simple as limiting the number of privileged accounts and limiting where, how, and when they can be used. And while they are not a trivial task to implement, the tools for supporting privileged access management are very effective and ultimately easy to manage. Accordingly, a sound re-evaluation of all cyber hygiene practices can prove to be a low-investment, high-impact undertaking. Closing unused ports, shutting off unneeded services, and limiting the infrastructure's exposure to the Internet where possible are highly achievable practices that can be catalyzed by the use of basic tools that identify such weaknesses.

Increasing situational awareness is another place where there can be high payoff. Infrastructure monitoring may take more up-front effort, but gives the organization better situational awareness of anomalies that allow them to act in a more timely manner, just as a solid vulnerability management program can inform about weaknesses before they are exploited.

Knowing that any good defensive action must be balanced with operational resiliency, including ransomware-specific scenarios in incident plans, as well as exercising such scenarios regularly, requires little investment and improves organizational awareness to such potential attacks. And, organizational awareness, especially through training and awareness programs, fortifies ground-level resistance to ransomware where the battlelines in the war on ransomware are often drawn and won.

In short, we believe that this back-to-basics approach takes some of the easily exploitable organizational weaknesses off the table for attackers. In the end, if an attacker wants something of value in the organization, making them work harder for it might just be the ultimate deterrent. Remember: ransomware attackers also must confront the economics of their activities. They will be less likely to invest in those attack vectors that have high investment and low payoff.

Recommendations

While our research findings certainly don't forecast a successful future in meeting the growing ransomware challenge, the good news is that there are a few key actions that an organization can take right now to substantially improve their ransomware defenses. Despite cyber criminals expanding the tools and techniques they use to increase the success of their attacks, an organization's effort to meet the attackers head-on is not entirely futile.

As our data indicates, a reframing of the organization's approach to ransomware can be achieved by focusing on cybersecurity basics. To that end, we recommend 5 important-but-simple actions that organizations should take now.

Assess your Commitment to Controlling & Securing Privileged Credentials.

Organizations should assess how well they are controlling the secured handling and use of privileged credentials. This includes taking an inventory of privileged credentials, justifying their need and use, and eliminating credentials where possible. Many organizations find the level of privileged credentials grow over time and may be assigned to personnel who no longer have a legitimate need or have left the organization.

If your organization is fortunate enough to be using a privileged access management solution, it's imperative that you confirm you are using all of the capabilities the solution provides, consistent with your organizational security requirements. This includes using the tool's vaulting capability, logging and recording the use of the credentials, and where possible, obfuscating the credentials so that they are not "knowable" by the user. Your PAM vendor is likely well-equipped to help you vastly improve the functionality of your solution in your unique operating context, so reaching out to them for help is a good start.

Improve the defensive posture of your operating environment.

Organizations do not always have the luxury of implementing defensive controls when deploying new infrastructure. And, with the constant rate of infrastructure changes driven by new functions and security updates, there is a good chance that basic hygiene has deteriorated over time.

It is always good practice to periodically assess the computing environment to ensure fundamental controls are in place and that defenses against ransomware infection are fortified. There are many tools available for performing a quick hygiene survey to help in this effort. This simple effort may identify services that should be turned off, discover open communication ports that should be closed, identify unnecessary exposure to the Internet, and highlight administrative capabilities that need to be reduced. And of course, the hygiene survey should confirm firewalls are properly deployed and anti-virus and malware protections are up to date. Finally, don't limit your hygiene check-up to the server and network infrastructure. The end-user environment needs the same level of attention to ensure only essential services are available, administrative capabilities are limited, and endpoint detection and response capabilities are strong.

Check-in on your level of supply chain risk.

Today, your organization exists in an ecosystem that connects you to a broader, and often less-controllable, operating environment. Determining your level of exposure to risk that may be inherited from your supply chain will help you build a roadmap for developing and implementing the right practices and controls to minimize this risk.

If you don't have a formal supply chain risk management program in place, it is a good time to identify your critical external partners—especially those to whom you have direct infrastructure connections—and gather information on the state of their cybersecurity controls. Many of these organizations routinely provide such information on request. Additionally, as you review access to your key systems and data assets, make sure that you include in your review potential external parties who may have access credentials. With constant organizational change, there's a high likelihood that there are former employees of your external partners who still have access credentials to your environment. And finally, with your critical vendors, perform a quick survey of where they may store, transmit, or process your critical data—and make sure to correct any deficiencies. Remember:your ransomware defenses are only effective if they cover your entire threat environment, which includes your external partners.

Maintain and update your ransomware incident response plan.

Incident response plans tend to gather dust over time and are often limited in coverage, especially as new threat vectors emerge.If your plan does not have a playbook specific to various ransomware scenarios, you may find your preparedness is less-than-sufficient. Developing a ransomware-specific response may require you to broaden the number of organizational stakeholders that are involved as well. For example, because ransomware often involves financial considerations, you may need to expand involvement to the CFO's office, insurance personnel, and legal. In some cases, you may need provisions to convene Board-level involvement. And, building a ransomware-specific playbook is not enough—you should schedule and execute an exercise of this playbook, even if you only do a quick table-read. This will help you find deficiencies in the plan and update accordingly.

Reassess your capability for managing vulnerabilities.

Vulnerability management confounds many organizations if only because of the sheer volume of vulnerabilities that require attention. Fortunately, a lot of exposure to ransomware can be neutralized by patching and updating, but only if this is performed in a timely manner.Review your current vulnerability management practices and processes to determine how long it is taking to resolve "critical" and "high" vulnerabilities on a timely basis. Tighten the time-to-remediate window to the shortest period that is operationally feasible. And scour your backlog—you may find that you have unremediated vulnerabilities in your queue that are over-exposing you to ransomware and need immediate attention.

Our Research

Axio has helped thousands of organizations to benchmark, plan, and manage their cybersecurity, risk management, and risk quantification programs. Our work with organizations across several critical infrastructure sectors—such as health, energy, utilities, financial, and manufacturing—focuses on improving cybersecurity through a risk lens that organizations can use to facilitate better cyber-defense decisions and allocation of investments.

A cornerstone of our approach is the Axio360 platform. Through the Cyber Program Planning and Management capability, organizations can use the platform to quickly assess their cybersecurity programs and build improvement roadmaps, aligned with common industry-accepted frameworks such as NIST CSF, C2M2, CIS20, and CMMC.

About our Authors

David W. White | President & Co-founder|dwhite@axio.com

David White leads Axio's innovation team and federal team and is actively involved with clients deploying the Axio360 software solution. He co-developed Axio's cyber risk management process and continues to refine the assessment, risk modeling, threat analysis, insurance analysis, and software solution that comprise that process. He has deployed the Axio360 solution with customers within the energy, utilities, financial, manufacturing, pharma, medical device, professional sports, and entertainment sectors. He served in a leadership role in the development of the Cybersecurity Capability Maturity Model (C2M2) versions 1 and 2 in support of the US Department of Energy and is a frequent speaker at board meetings, conferences, webinars, and other events. David co-authored the CERT Resilience Management Model (CERT-RMM) and was the chief architect for the Smart Grid Maturity Model (SGMM).

Richard Caralli | Cybersecurity Advisor|rich.caralli@outlook.com

Richard Caralli is a senior cybersecurity advisor with significant executive-level experience in developing and leading cybersecurity and information technology organizations in academia, government, and industry. Caralli has 17 years of leadership experience in internal audit, cybersecurity, and IT in the natural gas industry, retiring in 2020 as the Senior Director – Cybersecurity at EQT/Equitrans. Previously, Caralli was the Technical Director of the Risk and Resilience program at Carnegie Mellon's Software Engineering Institute CERT Program, where he was the lead researcher and author of the CERT Resilience Management Model (CERT-RMM), providing a foundation for the Department of Energy's Cybersecurity Capability Maturity Model (C2M2) and the emerging Cybersecurity Maturity Model Certification (CMMC). During his 15 year tenure at Carnegie Mellon, Caralli was also involved in creating educational and internship programs for master's degree and continuing education students in the Heinz College.