State of Ransomware Preparedness

Research Study: 2022

A Research Report

Executive Summary

The 2021 State of Ransomware Preparedness Report indicated that ransomware preparedness significantly lagged behind the rapid rise and evolution of ransomware attacks. In the 2022 follow-up to this report, Axio researchers again examined data from users of the Axio360 assessment platform to identify improvements in ransomware defenses, particularly in key areas of deficiency indicated in the 2021 report. The result: while some notable improvements have been made, ransomware preparedness continues to be insufficient to keep pace with new attack vectors.

The lack of basic cybersecurity practices and controls continue to undermine organizational attempts to improve ransomware defenses. In 2021, seven key areas of deficiency were noted, and again dominate the 2022 study results.

Key Findings

- **Insufficient progress is being made in implementing and maintaining foundational cybersecurity practices;** poor cyber hygiene and management of privileged credentials and access continues to over-expose organizations to ransomware.
- **Management of supply chain risk is not keeping pace with the rapid expansion of the threat surface** resulting from increased use of external parties for cloud-based infrastructure, applications, and services.
- **Incident management has not matured to address ransomware head-on** and to evolve from a discrete activity to a continuous process.
- **Basic network monitoring is improving,** but complementary controls such as network segmentation remain deficient.
- **Inadequate and inconsistent identification and remediation of known vulnerabilities** continue to provide hackers ample time to perfect and execute ransomware attacks.

Key Datapoints

- The number of organizations with a functional privileged access management solution in place increased by 10% but remains low at 33% overall.
- Limitations on the use of service and local administrator accounts remains average overall, with nearly 50% of organizations reporting implementing these practices.
- Approximately 40% of organizations monitor third-party network access, evaluate third-party cybersecurity posture, and limit the use of third-party software.
- Less than 50% of respondents implement basic network segmentation and only 40% monitor for anomalous connections.
- Critical vulnerability patching within 24 hours was reported by only 24% of organizations.
- A ransomware-specific playbook for incident management is in place for only 30% of organizations.
- Active phishing training has improved, but is still not practiced by 40% of organizations.

Introduction

In 2021, Axio issued the 2021 State of Ransomware Preparedness Report (2021 Study), a research study highlighting several concerning findings about the general state of organizational readiness to combat the evolving ransomware threat. The study was based on data collected from the Ransomware Preparedness Assessment, part of the Axio360 suite of assessment tools. The assessment reflects data collected from hundreds of ransomware events, guidance for DHS, and Axio's ongoing ransomware research, and includes essential cybersecurity practices needed for ransomware success.

At the time of the 2021 Study, over 100 organizations across multiple critical infrastructure sectors had used the tool to determine their cybersecurity posture against ransomware. Using de-identified data collected from organizations that completed the assessment, Axio researchers established patterns and emergent properties that provide insight into why organizations continue to be susceptible to ransomware attacks. These insights were published in the 2021 Study, along with several recommendations for improvement.

Ransomware dominated the conversation when the 2021 Study was conducted and published. The SolarWinds attack raised our consciousness of new ransomware attack vectors and methods, weakening our confidence in performing previously-routine tasks for maintaining and patching software. A flood of headline-producing attacks followed, notifying us that no sectors were to be spared as ransomware intrusions on agriculture services reminded us that these attacks were no longer just about collecting the ransom. Indeed, the new reality was one of intentionally causing wide-spread disruption, economic damage, and social unrest.

Indeed, the new reality was one of intentionally causing wide-spread disruption, economic damage, and social unrest.

Unfortunately, this does not seem to have had much effect on slowing down the rate and velocity of ransomware attacks. Nor has it blunted the innovativeness of the attackers. ThreatPost reminds us that easy access to corporate networks combined with a thriving market of “ransomware-as-a-service” tools are turning the modern-day version of script kiddies into next-level cybercriminals, fueling a 935% spike in organizations that had their stolen data exposed on a data leak site.

Research Methodology

Axio researchers analyzed updated data from the Axio360 Ransomware Preparedness Assessment tool to prepare the 2022 State of Ransomware Preparedness report (2022 Study). The Ransomware Preparedness Assessment is informed by input from hundreds of ransomware events, guidance from the U.S. Department of Homeland Security, and Axio's own research. Organizations across multiple critical infrastructure sectors have used the tool to determine the strength of their ransomware practices and controls, to identify gaps, and to prioritize improvements.

The Ransomware Preparedness Assessment contains 65 core practices arranged in 8 domains. Participants are asked to rate the implementation status of each practice in their organization using a four-point scale: Fully, Largely, Partially, and Not Implemented. Practices noted as Partially or Not Implemented are indicative of a lack of capability that may affect ransomware preparedness.

Using updated and anonymized self-evaluation data collected from assessment participants, Axio researchers identified emergent themes, as well as notable changes in the state of practice from the 2021 Study. The results are detailed in this report.

Key Observation

The results of the 2022 analysis confirm a persistent truth: **success in ransomware intrusion and organizational impact continues to be impeded by the failure to implement and institutionalize the most fundamental cybersecurity practices.** Ransomware attackers have indeed ramped-up their capabilities, but substantial defensive power can still be harnessed to strengthen resilience to attacks. The rise in the number and velocity of attacks observed in the past year will likely continue on an exponential trajectory, reinforcing the imperative for organizations to evaluate their basic, defensive practices and controls while commencing efforts to understand their potential ransomware losses in a quantitative context. Quantifying what's at risk might catalyze a new-found interest in making investments in foundational improvements.

In other words, there's a good chance that the next dollar spent on improving basic practices might help the organization avoid major ransomware-induced losses down the line.

What We Found

In our 2021 Study, we noted seven key areas where observed deficiencies in basic cybersecurity practices diminish resilience to ransomware attacks. While the 2022 Study indicates observable improvement across the board, overall performance continues to be average at best and warrants renewed efforts to master basic cybersecurity practices, especially as ransomware attack tools, techniques, and methods evolve at a faster rate.

Ostensibly, the results of the 2022 Study are encouraging. But stagnation in mastering core cybersecurity capabilities is a concerning trend given that adoption of basic cybersecurity practices is baseline expectation for operating safely in the Internet and cloud-enabled world.

Indeed, with the broad availability of cybersecurity frameworks, tools, and practitioners (not to mention ever-expanding regulatory requirements), the barriers to improved cybersecurity capability are fewer and may require not much more than a renewed commitment.

As confirmed by the 2022 Study, ransomware preparedness remains a factor of the degree to which improvements can be attained in:

- Managing privileged access
- Improving basic cyber hygiene
- Reducing exposure to supply chain and third-party risk
- Monitoring and defending networks
- Managing ransomware incidents
- Identifying and addressing vulnerabilities in a timely manner
- Improving cybersecurity training and awareness

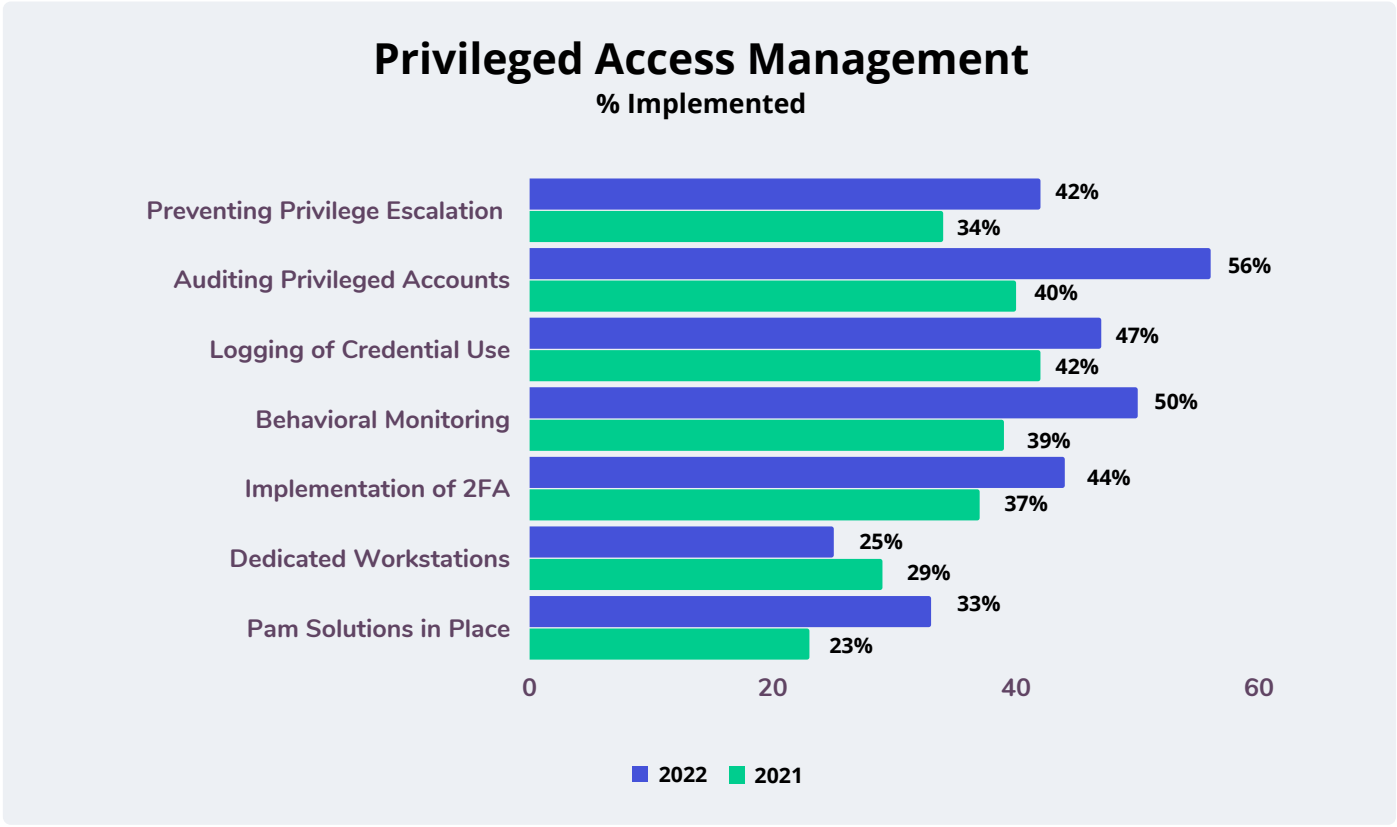
Managing Privileged Access

As in the 2021 Study, the management of privileged access continues to dominate the areas of weakness in ransomware preparedness.

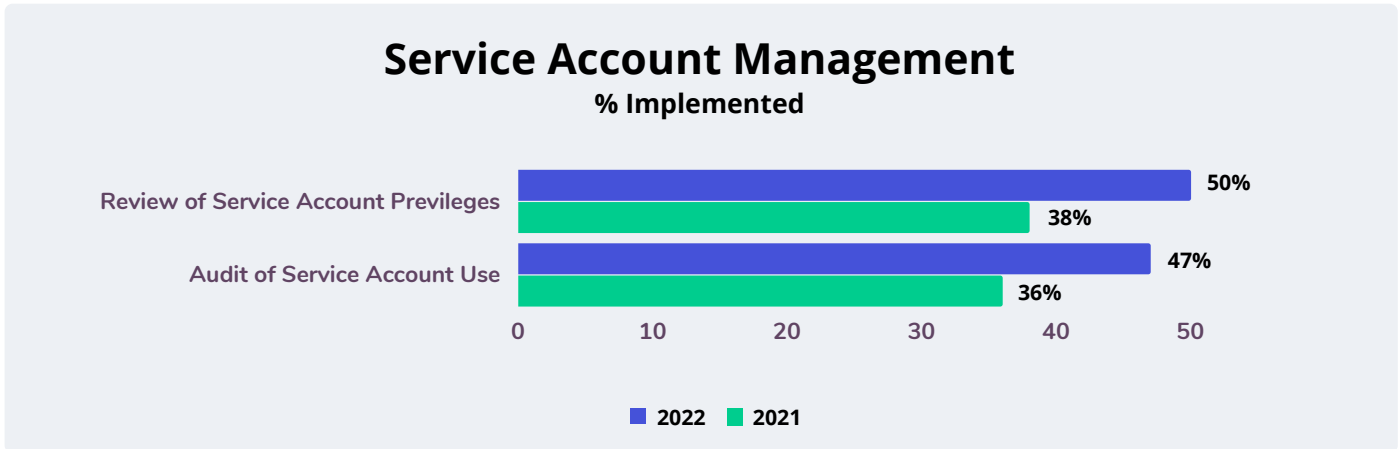
Privileged access management encompasses controls, practices, and supporting technologies that facilitate the administrative needs of privileged users in balance with reasonable limitations on excessive, inappropriate, and insecure use. Because privileged credentials are powerful tools for managing critical infrastructure, keeping them secure, in the right hands, and with appropriate use limitations is paramount. Ransomware attackers highly value privileged credentials as they not only enable the development and execution of ransomware campaigns, but may allow extensive infrastructure control, including the ability to obfuscate their tactics.

Results of the 2022 Study indicate that slightly more organizations are implementing dedicated tool-based solutions to control access to and track the use of privileged credentials. Additionally, the implementation of single-use credentials—disposable credentials that do not endure beyond a single use—is in place for 31% of organizations in the survey.

Analysis of the use of compensating controls for managing privileged access returned mixed results. The use of multi-factor authentication for privileged accounts improved slightly (+ 7%) while logging, monitoring, and auditing the use of privileged accounts increased more significantly, as shown in the chart below. However, restrictions on where privileged credentials can be used declined by 4% from the 2021 Study, indicating that the use of these credentials for purposes other than intended continues to occur. Additionally, the use of a tiered model for privilege escalation indicated a 9% improvement in the 2022 Study. This implies that more organizations understand the value of ensuring users of privileged credentials do not exceed the bounds of their authority and of limiting their ability to assign such credentials to other users who may not need such capabilities.



Similar findings apply to the secure management of service accounts. Service accounts are a type of privileged account that is broadly used to execute infrastructure services, typically without human intervention. These accounts have vast capabilities that are essential for sustained operations but can be very dangerous if exposed or captured. Use of these accounts by privileged users to perform administrative duties (often to bypass other controls) is discouraged because of potential mishandling and underscores the need to audit such accounts (and the functions they are authorized to perform) more closely. In the 2022 Study, improvements were noted in the percentage of organizations that regularly review service account privileges as well as audit the use of those privileges, with both nearing 50% implementation, as follows:



While there are clear areas of improvement in privileged account management, the use of automated solutions to enable stronger controls in this area remains low, and overall data suggests that the level of performance in this area needed to combat ransomware attacks that utilize privileged credentials remains insufficient.

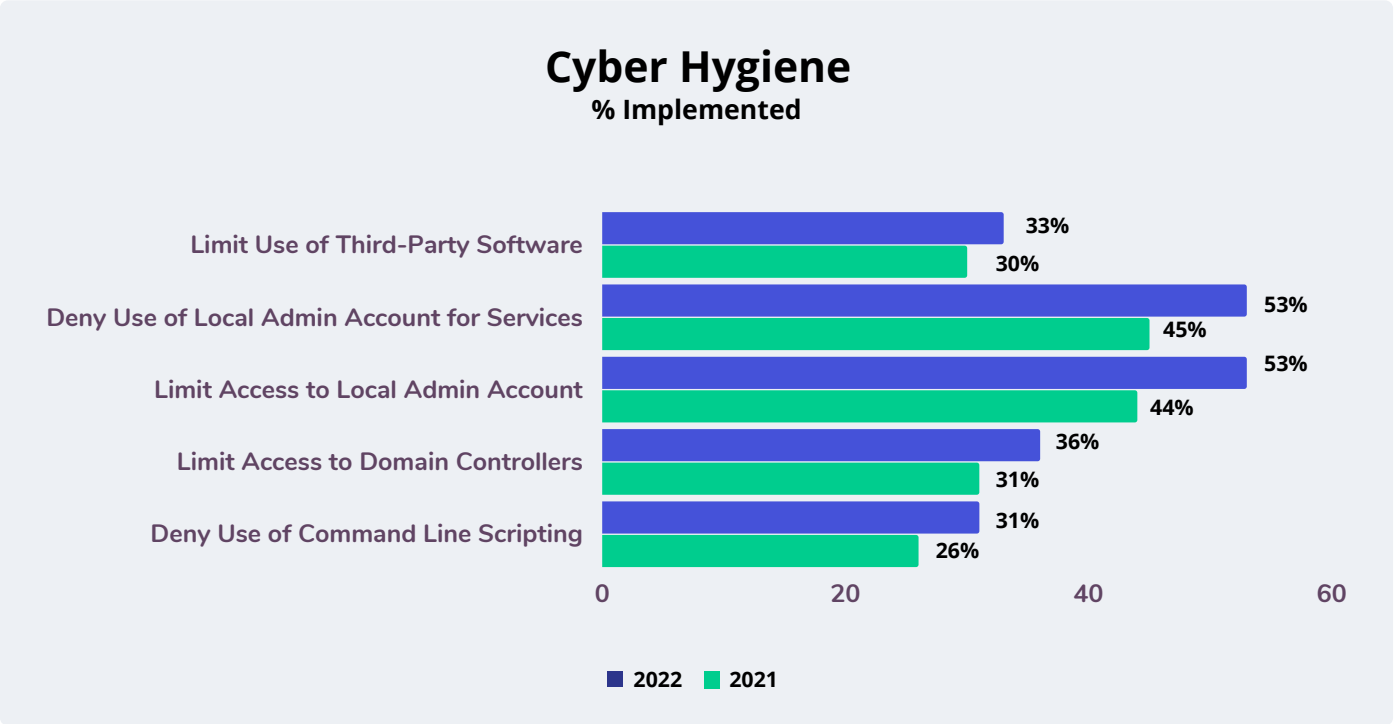
Basic Cyber Hygiene

The implementation of basic practices and controls to protect the "health" of networks, infrastructure assets, and data exhibited marginal improvement in the 2022 Study. Cyber hygiene is an essential preventative strategy for deploying and maintaining assets with a sufficient level of control that does not over-expose them to threats. This typically low-investment activity has a high potential payoff, especially if cybersecurity-focused asset builds and configurations are applied consistently and universally throughout the infrastructure.

Many of the weaknesses caused by poor cyber hygiene are highly controllable. For example, the use of command-line scripts can be restricted to authorized-use only, for a limited period, and not provisioned to general users if possible. Unfortunately, this practice showed little improvement (+5%) in the 2022 Study, with nearly 70% of organizations failing to implement it. Similar findings were noted with the practice of limiting domain controller access to the Internet. Because domain controllers can be used by attackers to facilitate the propagation of an attack, limiting exposure to threats is essential. Seventy-five percent of respondents continue to report they lack basic protections for their domain controllers.

Risks associated with the use of powerful local administrator accounts are also highly manageable. Yet, implementation of associated practices barely passes 50% in our data. This includes disabling local administrator accounts for general use and denying the use of these accounts to run services, such as for batch jobs or remote access, both of which are practiced by 53% of responding organizations. While this is an improvement over the 2021 results, it remains an insufficient level of achievement for a practice with little upfront investment and high payback.

Finally, the unabated use of third-party software continues. A slight increase of 3% of organizations in our data noted that they do not have exceptions or allow-listing processes in place to limit the acquisition and implementation of third-party software. Nearly 70% of organizations in the 2022 Study continue to allow the creation of a shadow technology environment that may be exposed to unknown and unmanaged threats.



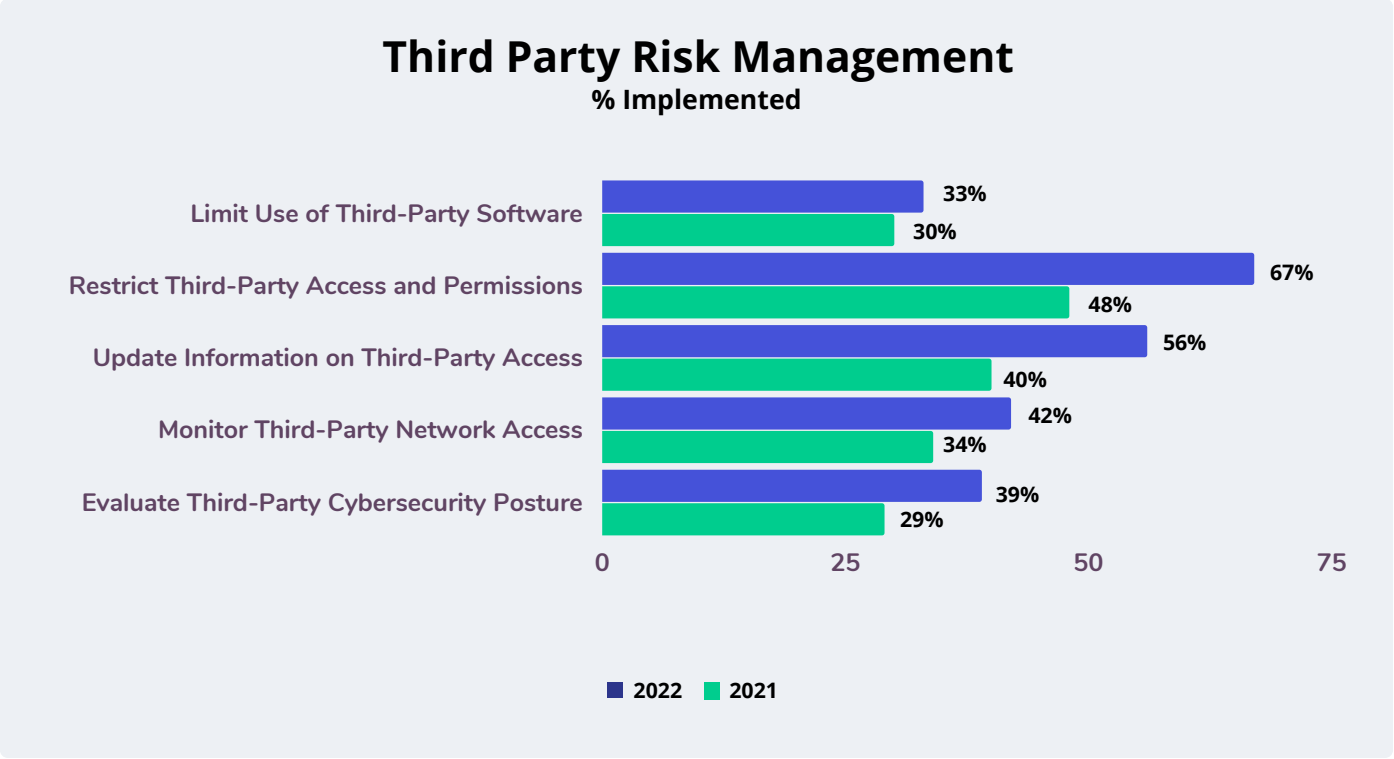
Supply Chain Risk Management

Exposure to ransomware continues to expand as the popularity of cloud-based computing and anything-as-a-service grows exponentially. The benefits of improved capabilities and reduced investment in infrastructure management come at a potentially high cost as the ability to directly control the threat surface is diminished. Attack vectors that once had little chance of success may now be solidly in the organization's risk profile—and ransomware attackers know this.

In the 2021 Study, we noted a significant over-exposure to potential inherited threats from external parties that could be reduced by adopting a few common-sense practices. The trend continues in the 2022 Study, although there is room for some optimism as adoption of basic third-party risk management practices appears to be on the rise.

For example, the number of organizations that regularly evaluate the cybersecurity posture of their third-party relationships has improved from 29% to 39%, with a corresponding 8% increase in organizations that monitor the cybersecurity posture of third parties to whom they have provided direct network access. Together, these activities provide better awareness of exposure to potential ransomware attacks that may be inherited through third-party relationships.

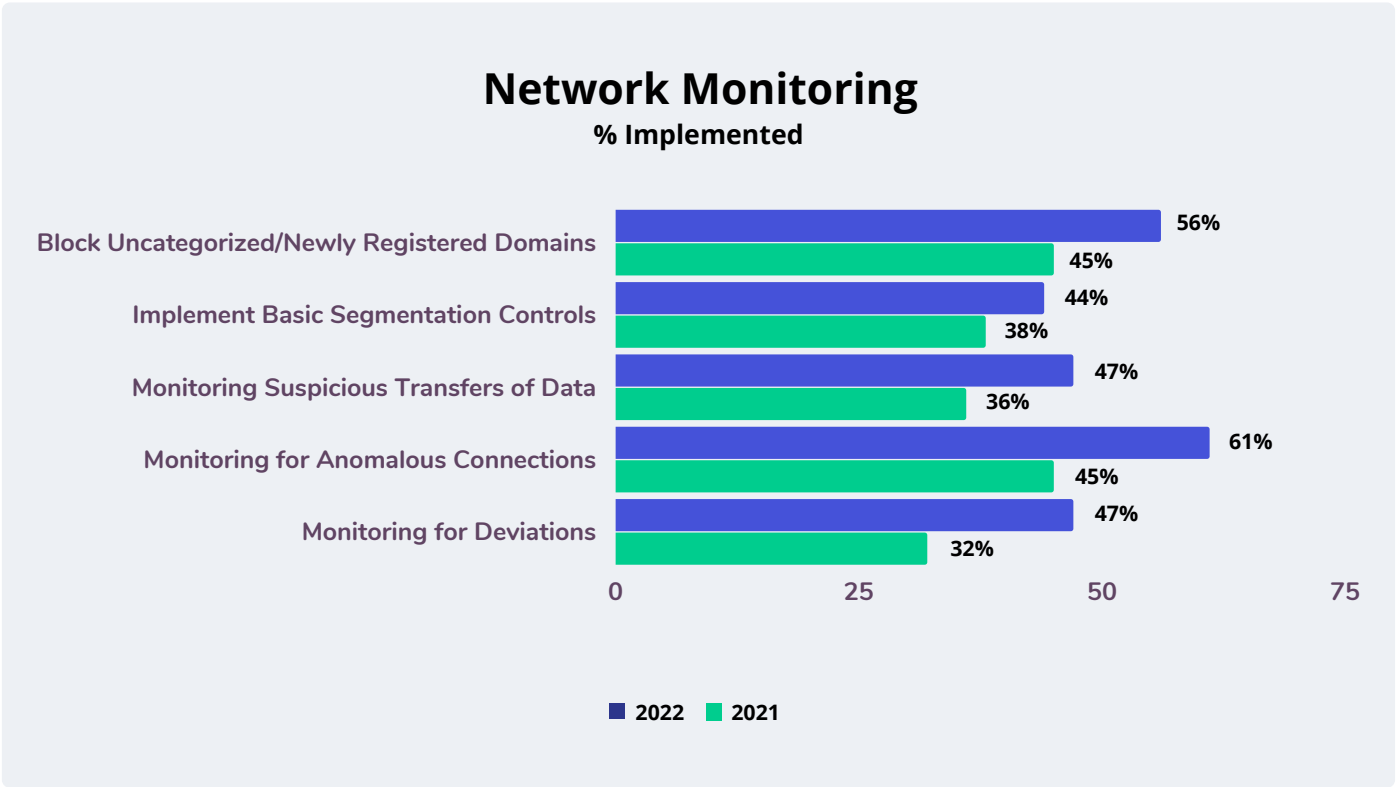
In addition, over half (56%) of respondents report that they regularly gather up-to-date information about external parties who have access to their networks, a rise of 16% over the 2021 Study. While this improvement is encouraging, newly emerging challenges raise further concerns. For example, the increased velocity of pandemic-driven staff turnover and shortages may manifest in higher levels of inappropriate use and sharing of credentials by third parties, requiring improved monitoring and use of compensating controls (such as imposing credential time restrictions and shorter expiration dates). And this message may be registering with more organizations: fully 67% of respondents have implemented controls to restrict account permissions and limit network access to specific segments, an increase of 19% from the 2021 Study.



Network Monitoring

By design, network architectures seek to facilitate high-quality, uninterrupted sharing of resources and data flow between users, systems, devices, and the outside world. But ironically, ransomware and other malicious content take advantage of these capabilities to propagate across the organization easily and quickly. Investments in basic network controls and monitoring remain essential for proactively identifying and neutralizing ransomware attacks.

The 2022 Study suggests the implementation of basic network controls is improving but may not be sufficient to reduce exposure to ransomware intrusion. Most notably, the implementation of basic network monitoring shows the most improvement. Forty-seven percent (47%) of organizations report monitoring for deviations from an established baseline of network and system activity, an increase of 13% from the 2021 Study. In addition, a 16% increase in organizations that monitor for anomalous network connections was noted, improving from 45% to 61% in 2022. Monitoring for suspicious transfers of data and processes that use excessive network resources showed similar improvements, as 47% of organizations now report this capability, an increase of 9% from the 2021 Study.



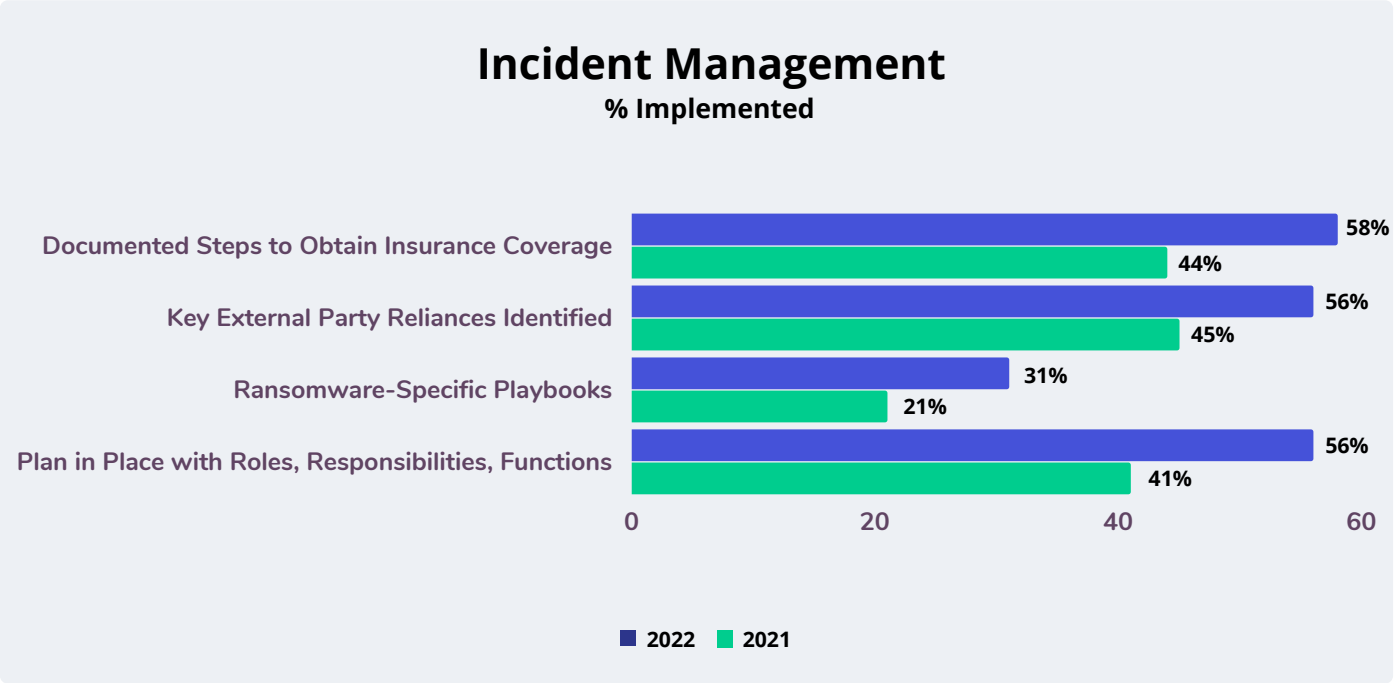
Measurable improvements in monitoring capabilities certainly fortify the detection of ransomware intrusions, but complementary controls such as network segmentation and blocking the sources of ransomware are equally necessary. Unfortunately, the implementation of basic segmentation controls continues to be underwhelming, with only 44% of respondents reporting that they deploy controls to limit and restrict the lateral movement of malicious actors once inside the network. While this is an improvement of 6% from the 2021 Study, the overall level of use of segmentation controls as a primary defense against ransomware attacks is alarming. Additionally, only 56% of organizations report using controls to block uncategorized and newly registered domains using tools such as DNS or web proxy filters, an improvement of 11%. While adoption of these complementary controls appears to be ramping up, existing levels indicate that ransomware attacks will continue to be successful and consequential.

Incident Management

The practice of incident management is an acknowledgement that a layered defense-in-depth approach does not provide guaranteed assurance that ransomware attacks sometimes break through and require decisive, planned, and timely action. High-profile attacks reinforce the need to include a specific ransomware-focused playbook in incident management plans, focused on threat containment and coordinated organizational response—with the intent to limit financial and reputational damage.

The practice of developing an incident management plan has improved significantly in the 2022 Study as nearly 56% of organizations responded that they had plans that detail specific roles, responsibilities, and key functions, an increase of 15%. However, only 31% of organizations include a ransomware-specific playbook in their plan. While this is an increase of 10% from the 2021 Study, clear improvement is required to ensure incident management is sufficient to address the specific challenges of managing a ransomware intrusion—including not only technical containment but organizational coordination to manage ransom demands, work with law enforcement, and limit potential reputational damage.

Managing a ransomware incident may also entail the orchestration of many external partnerships and knowing which key external partners and services are required during an incident could be vital to success. Fifty-six percent (56%) of respondents noted that they documented key external partners in incident management plans, an increase of 11% from the 2021 Study. And for organizations that procured ransomware insurance protections, 58% documented the steps necessary to obtain and preserve, a healthy increase of 14%.

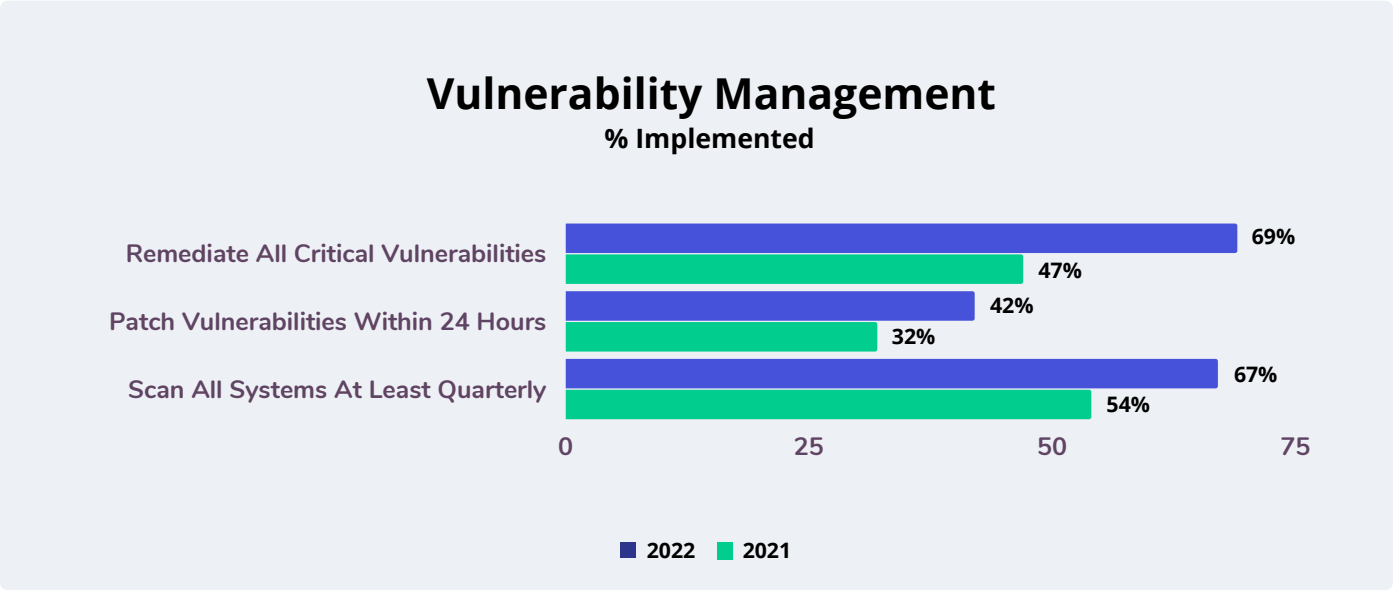


The emerging picture of ransomware incident management is certainly encouraging, but the lack of specific ransomware playbooks will continue to limit effectiveness.

Vulnerability Management

Timely identification of vulnerabilities and a shortened time-to-remediate continue to be essential to preventing ransomware intrusions. Organizations that fail to reduce vulnerability exposure time risk having attackers use that time to further perfect and weaponize their approach.

The 2022 Study suggests that the call for improving vulnerability management as a key approach to reducing ransomware intrusions is being heard. A majority of organizations (67%) now report that they scan all systems and applications at least quarterly, an increase of 13% from the 2021 Study. And while this is encouraging, even quarterly scanning can lead to unacceptable levels of exposure and time-to-remediate given the volume of vulnerabilities in modern systems, applications, and infrastructure and the velocity of ransomware attacks.



Unfortunately, the practice of remediating critical vulnerabilities, including the patching of vulnerable assets continues to evolve. Only 42% of organizations require critical vulnerabilities to be patched within 24 hours (an increase of 10% from the 2021 Study), with the objective of meeting this requirement more than 95% of the time. And, as was noted in the 2021 Study, some organizations still do not remediate all vulnerabilities with the potential for compromise, as 69% of respondents report meeting this objective. This is a significant increase of 22% over the 2021 Study but given that ransomware prevention is highly correlated to reducing exposure to known vulnerabilities, any achievement less than 100% signifies the battle against ransomware will not be won anytime soon.

Good News

In our 2021 Study, we established the barriers that are preventing organizations from reaching their potential for defending against ransomware intrusions. And while there is clear improvement across the board, much work remains to build better ransomware defenses.

In a few cases, our 2022 Study noted trends that may indicate organizations are finally taking the ransomware threat seriously and reconfiguring cybersecurity programs to account for the prominence of ransomware attack vectors. These trends include

Eighty-one percent (81%) of organizations reported they procured cyber insurance to respond to a ransomware event

Renewed focus on email as a primary attack vector, including controls to scan and block malicious email and providing processes for employees to report phishing attempts (94% and 89%, respectively)

Emerging controls over privileged account management including restricting access to domain controllers (86%) and limiting the population of users with domain administrator privileges (86%)

Performing data backup, offline storage, access controls, and encryption (75%)

Improving cybersecurity and awareness for email threats (72%) and conducting regular phishing exercises for users (61%)

High levels of implementation of basic network security practices including

- Anti-virus solutions incorporating behavioral analysis (practiced by 89% or respondents)
- Restrictions on unnecessary ports, protocols, services, and software (89%)
- Countermeasures against delivery of malicious payloads from websites (86%)
- Controls over potentially vulnerable services such as remote desktop protocol (83%)
- Routing of Internet traffic through security appliances such as DNS or web proxy filters (83%)

While these statistics are encouraging, the exponential growth of ransomware attacks demands that organizations consider these practices as requisite to their cybersecurity program, providing the foundation for improvement that will be needed to keep pace with ransomware innovation and velocity in the future. Indeed, as emerging attacks have demonstrated, ransomware attackers are not waiting for organizations to get the fundamentals right, and will continue to exploit program weaknesses to their advantage.

Recommendations

Ransomware as a commodity sets off alarms that ransomware attacks are likely to be persistent in the future. New ransomware attack vectors and the ease with which these vectors can be executed will demand mastery of basic cybersecurity practices and accelerate the need to adopt more mature controls. Investments in closing cybersecurity program gaps will become imperative, not aspirational.

As the 2022 Study suggests, there has been incremental improvement toward the goal of improving and sustaining baseline cybersecurity capabilities. But the program deficiencies highlighted in this report represent persistent weaknesses that result in cybersecurity risk that is largely controllable and manageable—and should be prioritized for investment. Closing these gaps remain a key imperative for managing ransomware.

To this end, we reiterate five important actions from the 2021 Study that should be considered to reduce ransomware exposure. However, realizing that ransomware risk cannot be 100% eliminated, there are additional actions that should be considered as new tools in the ransomware fight.

1. Control and Secure Privileged Credentials.

It is clear that privileged credentials expose organizations to risk if not limited and controlled. Over time, the use and proliferation of these credentials tend to grow while oversight wanes. Take an inventory of privileged credentials, re-justify appropriate use, and eliminate credentials where possible. Consider the use of a privileged account management tool and vendor to jump-start governance over these credentials.

2 . Improve Cyber Hygiene

Surveying the cyber health of operating infrastructure is imperative to identifying gaps that can be closed with limited investment and effort. Eliminating unnecessary exposure to the Internet, turning off unneeded services and access, and reducing administrative capabilities to a privileged few are actions that can significantly improve ransomware exposure. Imposing consistent architectural requirements on new operating environments can ensure new deployments are cyber-defensive from the start. A quick hygiene survey using commonly available tools can provide a quick report card from which to prioritize actions for improving cyber health.

3 . Reduce Exposure to Supply Chain Risk.

Ransomware defenses are only effective to the degree they cover the entire threat environment—whether or not in the organization's direct control. A formal supply chain risk management program aims to expand the organization's risk profile so that new and inherited risks from external dependencies are identified and incorporated into the cybersecurity program. A quick inventory of where data is stored, transmitted to, and processed by external partners can establish a third-party risk profile that informs the practices and controls that require attention.

4 . Practice Continuous Incident Management.

An out-of-date plan that gathers dust may turn out to be “no plan” when needed. As new threat vectors emerge, plans must be updated with new and revised playbooks to ensure sufficient organizational preparedness—including a ransomware-specific playbook, now considered to be a standard part of any incident response plan. And ransomware is not the last attack trend organizations will encounter. For this reason, viewing incident management as a continuous process ensures that the collective knowledge of the organization is used to inform and improve response—from regularly updating and exercising plans to rotating a variety of stakeholders through the process.

5 . Manage Vulnerabilities.

Managing vulnerabilities—from identification to remediation to elimination—is a critical success factor for reducing ransomware exposure. Patching systems, focusing on known critical vulnerabilities, and reducing the time-to-remediate window to the shortest period that is operationally feasible will significantly affect your ransomware attack profile. Remember: much of cybersecurity success involves blindly predicting what will happen in the future. Managing known vulnerabilities harnesses the power of hindsight, taking some of the guesswork out of the process.

Meet the Challenge Head-On

Fixing a problem starts with acknowledging its existence. An honest evaluation of program gaps is essential to prioritizing and remediating cybersecurity practices and controls that can fortify your ransomware defenses. And, in cases where you are forced to make a risk vs. reward decision, learning how to effectively communicate these trade-offs in language decision makers understand is critical. Axio can help with both.

How Effective is Your Ransomware Defense?

It's important to figure out where your cybersecurity program falls on the effectiveness spectrum. The Axio360 platform—which supplied the benchmarking data analyzed in this report—provides access to a variety of cybersecurity frameworks and tools that can identify program gaps and help to prioritize remediation activities. The platform includes assessment instruments for common frameworks like the Cybersecurity Capability Maturity Model (C2M2) and the NIST Cyber Security Framework (NIST CSF), and it also focused on instruments such as the Ransomware Preparedness Assessment. Assessment results can be prioritized and planned and tracked for remediation. And, your improvement path can be documented and communicated to stakeholders.

Will Your Cybersecurity “Bets” Pay Off?

Unfortunately, deciding which preventative measures to improve and in what order can be harder than it seems. While it is true that closing practice and control gaps should result in reducing the likelihood of a ransomware intrusion, control over materially affecting the probability of an event is limited at best. As a counterbalance, viewing an incident or event from the perspective of realized risk may be valuable for prioritizing and optimizing cybersecurity investments, if only because more precise calculations of risk vs. reward can be made.

Communicating program improvements in terms of quantifiable risk reduction can be powerful for transforming perceived threats into actionable plans supported by stakeholders and decision-makers alike.

Axio's Cyber Risk Quantification solution gives organizations the power to view ransomware (and other potential risks) in dollars-and-cents terms. Using a built-in scenario library, organizations can jump-start their quantification efforts by considering which scenarios are most relevant to their operational context. By understanding what's at stake in a scenario, plans and investments can be identified and visualized in terms of risk reduction and loss avoidance. Even the recommendations in this report can be viewed in simple quantitative terms. For example, if your cybersecurity program is deficient in managing third-party risk, scenarios representing potential inherited risk (such as a loss of critical data) can be developed and quantified, helping you to better decide if your third-party risk management program warrants investment and what type—improving defensive controls, improving operational resilience under attack, or both.

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, CIS18, and CMMC.

About our Authors

David W. White - President & Co-founder

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 U.S. 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 - Senior Cybersecurity Advisor

Richard Caralli is a senior cybersecurity advisor at Axio 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 at the Heinz College.