Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **October 2022**
Sponsored by **Asigra**, **BlackFog**, **Cyren**, **Infoblox**, **IRONSCALES**, **Micro Focus**, **SonicWall**, and **Trend Micro**

Ransomware Attacks: Strategies for Prevention and Recovery

Executive Summary

This white paper could start by reviewing the college that closed permanently after a ransomware attack[1] or the large school district that suffered an incident during a recent holiday weekend.[2] Or it could focus on how critical infrastructure—such as water treatment plants, pipelines, and meat processing plants—are increasingly under attack. We could even comment on the increase in ransom demands.

We are not going to do any of the above—at the beginning of this white paper or anywhere else. While there are important lessons to take from each of these situations, we will leave that analysis to others.

This white paper takes a different approach. It starts by quickly establishing the current context on ransomware before moving into an analysis of where current and best practices diverge. We'll look at eight areas where many organizations remain susceptible to ransomware attacks, outline new and emerging solutions or approaches that can be used to bolster controls and protections, and offer a report card for self-assessment by organizations. Most report cards are additive (the "better" level also requires the "baseline" controls, and the "best" level requires the controls from all three levels) while two are based on maturity (low, medium, and high).

The first four areas focus on defending against ransomware attacks, the final three focus on recovering after an attack, and the fifth area does double duty for defending and recovering. By the end of this white paper, decision-makers and influencers charged with evaluating and selecting cybersecurity solutions should have a better idea of their organization's readiness (or not) to counteract ransomware.

This white paper looks at eight areas where many organizations remain susceptible to ransomware attacks.

KEY TAKEAWAYS

- **Ransomware remains a threat—and a growing one at that**
  Threat actors are evolving their toolkits and playbooks to make ransomware more devastating to victims. Ransomware-as-a-Service (RaaS) and partner-in-crime models, along with greater supply chain specialization, increase the peril.
- **Metrics for ransomware attacks are both up and down**
  Some reports on ransomware show a threat with increasing frequency. Others show a downward trend. Sanctions imposed on Russia following its invasion of Ukraine appear to have neutralized the efficacy of Russian-based gangs.
- **Strengthen defenses against ransomware attacks**
  If 2022 is a "strategic pause" for ransomware attacks, organizations should increase security posture and decrease threat susceptibility for when ransomware gangs return to crime-as-usual.
- **Prepare to recover after a ransomware incident**
  While it is almost certain that every organization will face opportunistic attackers—and perhaps determined ones too—it is not certain that every organization will become a victim of a ransomware incident. But if that does happen, having a response protocol or recovery plan approved by the Board and ready to enact is invaluable. Lay a strong foundation now for recovery, if needed.

ABOUT THIS WHITE PAPER

This white paper is sponsored by Asigra, BlackFog, Cyren, Infoblox, IRONSCALES, Micro Focus, SonicWall, and Trend Micro. Information about each company is provided at the end of this paper.

Ransomware in 2022: Snapshot

Ransomware attacks are associated with a common set of realities in 2022. In brief:

- **Multiple levels of extortion increase the likelihood of a massive payday**
  Threat actors seek financial gain from ransomware attacks. It is bad news for the threat actor if the victim organization does not pay the ransom demand. To increase the likelihood of receiving a payment, threat actors have innovated beyond malicious data encryption as the sole blackmail lever. Additional levers include threatened distributed denial of service (DDoS) attacks and data exfiltration through hard-to-detect mechanisms like DNS tunneling with threats to sell, publish, auction, or otherwise disclose the stolen data if the ransom is not paid. Victim organizations may be able to address the operational disruption of malicious data encryption through backups, but mitigating risks associated with DDoS and exfiltrated data is a different challenge entirely.

- **RaaS and partner-in-crime models expand the number of attackers, ransomware variants, and advanced threat methods**
  Threat actors are making ransomware toolkits easily available to wannabe threat actors, speeding up their time to crime. Today's toolkits offer advanced evasions, exploits, and other techniques that were previously available only to nation-state actors or large cybercrime and ransomware gangs. When a new entrant threat actor lands a successful attack using a RaaS toolkit, any ransom payment is divided between the threat actors. RaaS has been implicated in increasing the number of ransomware attacks. The number of ransomware variants in the first half of 2022 doubled compared to the second half of 2021.[3]

- **Ransomware supply chain models amplify specialization through division of labor**
  Ransomware gangs are embracing specialist skills in crafting ransomware attacks, such as Initial Access Brokers (IABs) who sell access to compromised networks or devices, and post-compromise negotiators fluent in the language of the victim organization to negotiate the ransom payment. Ransomware gangs seek the same benefits from specialization and division of labor that the world has seen in most other business endeavors, such as manufacturing.

- **The most common entry points for ransomware are phishing (for credentials), open network ports and virtual private networks (VPNs), and vulnerabilities in applications**
  Distracted employees clicking malicious links, misconfiguring a device, or forgetting to apply a critical security patch continue to be the leading causes of most breaches. Email is still the top attack vector so businesses must evolve their thinking beyond email perimeter defense and user training. Insufficient protections against these attack entry points is like painting a target on the front door.

Ransomware in 2022 features multiple levels of extortion, RaaS models, and rampant data exfiltration.

- **Paying the ransom is expedient, but often ineffectual**
  Many organizations pay the ransom demand to gain the decryption key, stop the publication of exfiltrated data, or prevent a DDoS attack—despite low success rates. Cyber insurance cover is a leading source of funding for paying ransoms. However, decryption keys don't always work to restore encrypted data and cyber criminals still leak data. Paying the ransom to recover from an attack has four significant weaknesses. First, it doesn't address the systemic shortcomings that allowed the attack to succeed. Second, it funds additional cyber crime. Third, future cybersecurity insurance premiums will be higher—assuming coverage even remains available to the organization given their changed risk calculus. Finally, it often leads to additional attacks or subsequent ransom demands for exfiltrated data because threat actors know the organization has a proclivity to pay up.

- **Just one unaddressed entry point is enough for an attack to gain a foothold**
  Ransomware attacks start with one successful phishing email,[4] access to a single password to a legacy VPN that isn't using multi-factor authentication (MFA),[5] or abuse of a newly identified or unpatched software vulnerability. The problem has been exacerbated due to visibility challenges stemming from the transition to a more hybrid workforce over the past couple of years.[6] Hoping that threat actors will not trick employees, find infrequently used systems, or attack irregularly patched applications has repeatedly proven shortsighted.

Many organizations pay the ransom demand to gain the decryption key, stop the publication of exfiltrated data, or prevent a DDoS attack—despite low success rates.

Are Attacks Increasing or Decreasing?

Several reports suggest ransomware attacks are increasing in 2022:

- **August and September 2022 were two of the three worst months for ransomware incidents since January 2020**
  BlackFog tracked 39 ransomware reported incidents during August[7] and 33 in September,[8] two of the three highest numbers recorded since January 2020. In July, BlackFog concluded that many incidents were going unreported, since public notification of incidents were decreasing while attacks were increasing.[9]
- **Increased activity among RaaS threat actors during 1H 2022 vs. 1H 2021**
  Trend Micro's 2022 Midyear Cybersecurity Report shows significantly higher ransomware detections from several threat groups, including LockBit (5x higher), Conti (almost 2x higher), and BlackCat (a new group at the end of 2021, but already with 75% the number of detections as LockBit).[10] Competition between RaaS threat actors will spur the development of improved toolkits.
- **Living through the 'golden era' of ransomware**
  European authorities said the world was facing the golden era of ransomware, based on an analysis of incidents from April 2020 to July 2021 (which increased by 150%).[11] They warned that ransomware was likely to get worse before the era ends, calling it the "prime threat" facing organizations as cyber criminals follow the money to profitable criminal activity.

Ransomware is the "prime threat" facing organizations as cyber criminals follow the money to profitable criminal activity.

Other reports indicate attacks are trending downward. For instance:

- **23% decline in ransomware attacks in 1H 2022**
  The mid-year update to the 2022 SonicWall Cyber Threat Report shows a 23% decline in the number of ransomware attacks from January 2022 to June 2022 compared to the same time period in 2021 (236.1 million in 1H 2022 vs. 304.7 million in 1H 2021).[12] While that is good news, SonicWall offers the context that the volume of ransomware in 1H 2022 is already higher than the full-year totals for 2017, 2018, and 2019, and is 77% of the way to reaching 2020's full-year total.
- **7% decline in 2Q 2022 vs. 1Q 2022**
  The number of ransomware victims tracked per month decreased by 7% from Q1 (232 victims per month) to Q2 (216 attacks per month).[13]
- **NSA on declining ransomware attacks**
  Russia's invasion of Ukraine has disrupted operations of ransomware threat actors and gangs, many of which operate in Russia.[14] The National Security Agency (NSA) in the United States says that financial sanctions make it more difficult for Russian gangs to capture ransom payments and purchase infrastructure to run new attacks. It is uncertain when the invasion will end, and it is uncertain to what degree and with what speed the sanctions will be lifted when it does. But the net current effect is a decline in the ability of the ransomware ecosystem to perpetuate new attacks.

One interpretation is that 2022 is a "strategic pause" in ransomware attacks. However, irrespective of whether attacks are increasing or decreasing, organizations should strengthen what is working and address what is not. When attacks are increasing—in frequency, sophistication, and damage potential—urgency is high for rapid mitigation. When attacks are decreasing or paused, there is an opportunity for a more thorough readiness review. Doing so increases security posture and decreases threat susceptibility.

Ransomware SWOT

In this section, we present a SWOT on ransomware in 2022.

STRENGTHS

- **Wider understanding of the ransomware threat**
  General awareness of the ransomware threat is much higher than five years ago, and many organizations have made good progress in mitigating outstanding vulnerabilities and weaknesses that were open to attack.
- **Higher systemic preparedness**
  Protections that address ransomware-specific threats create wider protections against other types of cyberattacks. For example, stronger forms of MFA reduce the likelihood of network breaches in a ransomware attack, as well as decreasing vulnerability to phishing attacks. Likewise, investments in zero trust, least privilege, and network segmentation have strengthened network security—and hardened defenses against ransomware.

WEAKNESSES

- **Ransomware attacks are still evolving and successful**
  Ransomware attacks continue to turn into incidents, affecting organizations across all industries. New vulnerabilities and exploits amplify this challenge.
- **Preparedness against key entry points is lacking**
  While organizations have made some progress in strengthening protections against ransomware, many hold back from embracing stronger protections until after suffering a devastating incident and senior management feeling the gravity of the risks enumerated by security leaders. Almost all organizations promise to strengthen identity and embrace MFA in their press release after an incident.

Many organizations hold back from embracing stronger protections until after suffering a devastating incident.

OPPORTUNITIES

- **Embrace the opportunity of the strategic pause**
  Use the current strategic pause in ransomware attacks to strengthen defenses, plug gaps in visibility, address vulnerabilities, and decrease the likelihood that a future attack will succeed.
- **Decrease relative attractiveness of attacking your organization**
  Protecting against ransomware requires pursuing two outcomes: decreasing the attractiveness of each organization as a target relative to all other organizations and decreasing profitability of ransomware as a criminal endeavor. The first outcome can be pursued directly; the second only indirectly.

THREATS

- **Retaliatory damages**
  Ransomware gangs hampered by sanctions and seeing fewer successful attacks for their efforts may inflict greater damage, escalate ransom demands, and impose retaliatory long-run effects on the few they do compromise. For example, they may pivot from malicious data encryption to permanently wiping data or destroying physical control systems. Further, once the invasion of Ukraine ends, Russian gangs are likely to significantly increase their attacks to regain profits lost during the conflict.
- **Increasing rates of data exfiltration**
  Virtually all ransomware incidents include data theft to increase the likelihood that the ransom demand will be paid.[15] Threat actors use stolen data in serial ransom demands. Too few organizations consider protections against data exfiltration as a mandatory part of their cyber toolset.

1. Strengthen Identity Methods

Account credentials provide access to systems, applications, and devices—unlocking a set of access privileges depending on the user for whom the credential is intended. But a username and password are associated with an individual only indirectly; there is nothing that directly binds the credentials to an individual. Credentials can be compromised through credential stuffing attacks or by tricking an employee into giving up their credentials through a phishing email. This allows a threat actor to present themselves to systems, applications, and devices as the employee. Phishing is a frequent precursor to ransomware attacks, because ownership of an email account establishes a trusted identity that can be used to reset passwords to other systems, or phish other employees and vendors. Strengthening identity with MFA is almost always undertaken with urgency and a sense of mea culpa after a ransomware incident.

SOLUTIONS FOR STRENGTHENING IDENTITY

MFA requires multiple forms of authentication before access is granted. MFA links something the individual knows (the username and password) with something they have. The "have" part is provided through a separate device when needed. Basic forms of MFA rely on codes sent by SMS or email, but these have proven vulnerable to compromise. A threat actor can access these codes if they have compromised the email account or succeeded with a SIM-swapping scam. Stronger options are:

- **Shift to stronger forms of MFA**
  Stronger forms of the "have" part of MFA include one-time passcodes generated by Authenticator apps on mobile devices and FIDO-based hardware keys. While these forms are much stronger than codes sent by SMS or email, they have two shortcomings. First, unless biometric checks are also required (such as a facial scan on a device), mere possession of the mobile device or hardware key by a threat actor still enables identity theft. Second, many phishing kits can capture and leverage codes from authenticator apps.
- **Use biometric authentication to tie identity with a specific person**
  While MFA relies on a "have" for the second factor, biometric authentication relies on an "are" factor. Assuming non-commodity solutions are used to create and confirm biometric indicators, voice prints, fingerprints, and face scans enable unique identification of an individual. Embracing stronger forms of identity decreases the opportunistic threat of compromised credentials by significantly increasing the difficulty of abusing stolen credentials.
- **Embrace risk-based authentication**
  Authentication based on the strongest forms of identity will sometimes not be enough. Other risk factors beyond the identity—the type of device used, the network connection, when access occurs, and the geographical location of the access request—can signal greater need for caution in granting access at all or in varying gradients. Solutions that unlock visibility into these signals enable the use of additional authentication and verification checks when risk is high.

Embracing stronger forms of identity decreases the opportunistic threat of compromised credentials by significantly increasing the difficulty of abusing stolen credentials.

REPORT CARD FOR STRENGTHENING IDENTITY (MATURITY)

Grade	Indicators
Low	Username and password with basic forms of MFA
Medium	Stronger forms of MFA such as Authenticator apps and hardware keys
High	Biometric authentication plus risk-based authentication

Source: Osterman Research (2022)

2. Act on Internal Threat Signals

Stopping ransomware from establishing a foothold inside the organization's systems is an essential cybersecurity strategy, but it cannot end there. If ransomware does slip through defensive armaments, neutralize it before it causes damage. Having the visibility to continuously identify and respond to internal threat signals is part of a comprehensive defensive strategy.

SOLUTIONS FOR INTERNAL THREAT SIGNALS

Solutions that enable detection and mitigation of internal threat signals include:

- **Ensure visibility of internal attack surface**
  Endpoint detection and response solutions (along with newer variants) profile applications running across the IT ecosystem to provide visibility on what employees are using and how widely. This enables rapid detection of vulnerable applications, versions, and processes considering new threat data. Such solutions also support detection of lateral movement before ransomware is detonated. After gaining an initial foothold on one device through compromised credentials or exploiting a vulnerable application, threat actors attempt to install malware and hacking tools as widely as possible. The more widely pre-detonation malware is installed, the more crippling the attack when it is denotated. While this process of lateral movement is stealthy it is not invisible, hence if detected, it can be mitigated before the malware is detonated.

- **Automate detection of and response to mailbox threats**
  Attackers have mastered the ability to deliver threats to employee inboxes and trick distracted employees into clicking a malicious link. Managing this problem of evasive and sophisticated email attacks requires coordinated optimization across detection methods, user participation, automation, and security analysts. Achieving a mature approach to targeted email attacks requires automating processes, shifting from prevention to incident response, modernizing user training to apply it to current attacks in real-time, and leveraging managed services to reduce alert fatigue and email security configuration errors by security analysts.

- **Monitor baseline deviations to detect insider threats**
  At least one ransomware gang is actively recruiting employees to become turncoats and provide surreptitious access to the IT systems of their organization as the entry point for a ransomware attack.[16] User and Entity Behaviour Analytics (UEBA) solutions create a baseline of normal behavior. These solutions track access patterns for employees—individually and in context of the group/department they belong to—and can throw off early warning signals when an employee's normal baseline is subject to sudden, strange, or unexplained variations.

- **Interrupt communication with command-and-control infrastructure and data exfiltration activity as it is happening**
  Prior to detonation, ransomware needs to communicate with its command-and-control infrastructure. Anti-Data Exfiltration (ADX) solutions identify outbound communication attempts from pre-detonation ransomware to this control infrastructure. Once identified, ADX solutions enable communication attempts to be disrupted, and by implication, the receipt of any returning commands to be eliminated. Such solutions should monitor outbound traffic from endpoints to identify abnormal behavior in traffic patterns and signals of compromise that are reflective of malware, ransomware, and other suspicious

Lateral movement is a stealthy but not invisible process: Detection enables pre-detonation mitigation.

processes. These include endpoint processes that were not designed to initiate network traffic, communication attempts with ransomware hotspot locations (such as Russia, North Korea, and China), and reliance on dark web protocols.

- **Stop malicious data encryption as it is happening**
  Solutions that detect the detonation of malicious data encryption can halt ransomware in its tracks. As soon as malicious encryption is detected, such solutions stop it and restore encrypted files to their pre-encrypted state, as well as triggering high urgency alerts about the detected ransomware activity.
- **Leverage network data for security visibility and control**
  Network visibility helps defenders who find themselves caught between the evolution of ransomware evasion techniques and the explosion of devices—such as bring-your-own-device strategies (BYOD), the Internet of Things (IoT), industrial control systems (ICS), and operational technology (OT). DNS-level defenses counter spoofing, lookalike domain names, DNS tunneling, and other evasion techniques both on and off-network. Some attacks simply use DNS since it is mostly unmonitored by secure web gateways (SWG), next-generation firewalls (NGFW), and other defenses. Tools like IP address management (IPAM) can provide responders with on-demand access to critical device details—such as platform and operating system details—to help prioritize and frame effective responses.

DISCUSSION

There are too many threats across too many vectors to delegate primary responsibility for acting on internal threat signals to cybersecurity staff, whether internally or at a managed services provider. No organization can afford the time or money to hire enough staff to manually address all ransomware threats across all elements of their IT ecosystem—networking components, servers, endpoints, and cloud services. The primary workflows for detection, neutralization, mitigation, and incident response across the breadth of the IT ecosystem must rely first on advanced automation. This has two implications:

- Cybersecurity staff complement these workflows and make decisions or judgment calls when needed in automated processes.
- Solutions that capture internal threat signals but require security analysts to take action are less valuable than solutions closer to the fully automated end of the continuum.

The indicators in the report card are additive since they work together to assure overall security.

The primary workflows for detection, neutralization, mitigation, and incident response must rely first on advanced automation.

REPORT CARD FOR INTERNAL THREAT SIGNALS (ADDITIVE)

Grade	Indicators
Baseline	Solutions that automatically interrupt early-stage communication with command-and-control servers, stop data exfiltration and malicious data encryption activity, prevent the delivery of threats to employees through email, and automatically mitigate vulnerabilities detected across endpoints, servers, cloud services, and more
Better	Detect and respond to inbox and insider threats or compromise
Best	Visibility into endpoints, servers, cloud services, and more for human-driven analysis of potential weaknesses, vulnerabilities, and egress points

Source: Osterman Research (2022)

3. Extend Threat Intelligence

Threat intelligence collates and synthesizes details of current threat activity experienced by a cohort of organizations. Vendors, governments, open-source groups, and others offer threat intelligence resources to provide early warning signals on current attacks, pending targets, and vulnerabilities that are actively exploited or otherwise high risk. Threat intelligence is based on the principle that if attackers are doing it, planning it, or know about it, organizations must too. It is imprudent for organizations to have less visibility than attackers.

SOLUTIONS FOR EXTENDED THREAT INTELLIGENCE

Solutions to explore for extending threat intelligence:

- **Hunt for threats across your ecosystem**
  Proactive threat hunting is the practice of looking for cyber threats that have gained an early foothold in your ecosystem. Threat hunting correlates parameters from multiple sources to identify the origin, type, and frequency of an attack. Leveraging aggregated data signals from multiple organizations makes it possible to obtain detailed insight into each identified threat, so that organizations stay ahead of cybercriminals as the threat landscape evolves. Threat hunting tools and services enable organizations to identify false positives, investigate threat origins, and provide peer-based risk analysis.
- **Monitor the external attack surface**
  Threat actors seek to discover and exploit weaknesses in the ecosystem, systems, and applications they can access. Government agencies offer complimentary external attack surface monitoring to certain organizations, and insurance providers are using these same tools to assess risk when evaluating coverage levels and setting premiums.[17] Since it is becoming an accepted part of assuring and assessing defensive posture by government agencies and insurance providers, it is the type of capability that organizations should be using themselves. Organizations that embrace solutions and/or managed security services that offer proactive and continuous external attack surface monitoring are more likely to stay ahead of threat actors in identifying weaknesses to mitigate and vulnerabilities to address. When threat actors can see what organizations cannot, attackers have a strategic advantage.
- **Track emerging threat indicators on dark web forums**
  Chatter on dark web forums offers early warning of potential attacks. Threat actors, particularly IABs, offer to sell access to networks or devices at newly compromised organizations. While company names are not disclosed in the sale notice, attributes of the compromised organization are listed. Some threat intelligence services are finding a modicum of success in correlating attributes with a given organization.[18]

If threat actors can see what organizations cannot, attackers have the strategic advantage.

REPORT CARD FOR EXTENDED THREAT INTELLIGENCE (ADDITIVE)

Grade	Indicators
Baseline	Threat intelligence services
Better	Threat hunting for deep intelligence and prevention
Best	External attack surface monitoring and dark web forum monitoring

Source: Osterman Research (2022)

4. Human Layer of Defense

People play a key role in protecting the organization from ransomware attacks by having the ability to detect suspicious phishing messages and other social engineering attempts, for example when someone from the "IT help desk" calls and asks for the employee's password or MFA code. Another part of this role is actively embracing the security protections required by the IT or security team to safeguard the organization, such as use of biometric hardware tokens. While people must never be treated as the only means of defense, they play an essential role as one of the defensive layers.

SOLUTIONS FOR CREATING A HUMAN LAYER OF DEFENSE

Creating a human layer of defense relies on the following approaches:

- **Offer better security awareness training**
  Forewarned is forearmed, and enlisting employees, managers, and executives in the war against ransomware is a must. Many organizations continue to offer security awareness training too infrequently and too rigidly to be helpful. Employees view such training as a check-box activity and remain disengaged—to the detriment of the organization. Static curriculum, exams, and fake phishing emails haven't stopped users falling for mailbox threats. Better security awareness training is characterized by relevancy to the individual and group, teachable moments, and frequency of small learning chunks. It must also address signals of an in-progress attack, such as receiving unexpected MFA prompts.[19]
- **Test the training and act on the quantified risk**
  Training on security and testing the efficacy of that training are two sides of the same coin. Platforms that offer training content should also include testing capabilities to evaluate which individuals and groups struggle to apply the concepts. Testing approaches include phishing simulation, employee susceptibility to USB thumb drives "dropped" in the company parking lot, and penetration testing of facilities and offices. Learnings from these tests quantify current risk and provide insight for subsequent training and education initiatives. Distraction is a risk, too, and one that security awareness training often ignores.
- **Close the loop with employees on reported threats**
  Part of security awareness training is establishing the organizational processes for employees to report suspicious emails, particularly suspected phishing emails that are often a precursor to credential compromise and ransomware gaining a foothold. But it is what happens after they click the button to report the email that really counts. If an employee hears nothing back from the IT or security group that receives reports of suspicious emails, what does that mean and what should they do? Ensuring the IT or security group is sufficiently resourced is essential. This requires sufficient personnel, as well as optimal tooling that automatically distinguishes malicious reported emails from the benign, remediates malicious messages across all email inboxes, and closes the loop with employees.

People must never be treated as the only means of defense against ransomware, but they play an essential role as one of the defensive layers.

REPORT CARD FOR A HUMAN LAYER OF DEFENSE (ADDITIVE)

Grade	Indicators
Baseline	Relevant, context-aware security awareness training
Better	Training efficacy is regularly tested and evaluated
Best	Reported threats are mitigated promptly; training infused with current topics and is applied to real-time threats

Source: Osterman Research (2022)

5. Add Resiliency to Data Backup

A primary goal of ransomware attacks is monetary gain. Threat actors design the attack so that the victim organization pays the ransom to recover their data promptly. Backups have proven an effective countermeasure for organizations, since access to backups means systems, applications, and devices can be recovered without paying the ransom. For this reason, threat actors have extended their toolkits and playbooks to gain access to, delete, and corrupt backups by ensuring dormant ransomware is backed up, too. One study found that backup repositories were targeted in 94% of ransomware attacks and at least a portion of repositories were impacted in 68% of incidents.[20] If ransomware gangs pivot to using data wiping malware rather than just data encryption malware, backups will become critical to recovery—as paying a ransom for the decryption key is no longer an option when the data has been wiped.

SOLUTIONS FOR RESILIENT DATA BACKUP

Many organizations have a backup strategy, but only a minority successfully recover their data after a ransomware attack. Organizations that want to avoid downtime, streamline recovery, and not cave to paying the ransom to get their data back should be looking at the following solutions:

- **Test that backups work and enable restoration**
  Only one third of organizations can recover 80% or more of their data after a ransomware incident.[21] Betting the future of the organization on backups that don't enable full recovery within a short period of time is more costly than doing it right in the first place. If backups are going to be part of an organization's strategy against ransomware, they need to work, have been subjected to repeated testing, and support recovery dependencies between systems.
- **Use ransomware-aware intelligent backup and restoration procedures**
  Backups don't help in recovering from a ransomware attack if backups are riddled with dormant ransomware ready to denote upon restoration. Restoring non-encrypted business files along with dormant ransomware from infected backups merely enables the ransomware attack cycle to start again. Backup solutions need the intelligence to differentiate between business files and ransomware exploits if a clean backup is to be created or restored. All data should be scanned for malicious code during backup procedures and checked again during data restoration processes.
- **Elevate controls over changing backup settings and deleting data**
  Stronger identity controls are needed for approval and confirmation of significant requests against backup repositories. These added controls thwart threat actors who manage to compromise an administrator's account from maliciously changing backup and retention settings, or deleting backup data.

Threat actors have extended their toolkits and playbooks to gain access to, delete, and corrupt backups with dormant ransomware.

DISCUSSION

Adding resiliency to data backup does double duty for defending against and recovering from a ransomware attack. It is a defensive strategy because resilient data backups mitigate the threat of devastating consequences from a ransomware incident by safeguarding business data. It is also a recovery strategy, because if the organization is compromised through a ransomware incident, resilient backups provide a mechanism for restoring business data without paying the ransom for a decryption key.

The emphasis with resilient data backup is the backup of data in a resilient way, which is more than just the backup of data stored on servers in a resilient way. Data must be incorporated into backup processes wherever it is stored, so that the full complement of data required to operate business processes and meet archiving and compliance mandates are met. Designing backup processes so that only servers are included will by design exclude all data created on endpoints that is not synchronized to a server or cloud service.

Business data created by employees on laptops and mobile devices that is stored independently of a sanctioned business system will be ignored in backup processes if these endpoints are excluded. Such data can include notes from client meetings, early-stage product design ideas, and draft business reports. The shift to remote and hybrid working arrangements over the past several years means that almost all organizations will have business data stored on employee laptops and other devices that is not stored elsewhere.

Backing up data using multiple storage methods is different from backing up servers or endpoints using multiple storage methods. The first focus on the data, the second on backing up a particular manifestation of that data. If authoritative business data is distributed across multiple locations, the resilient data backup strategy in its defensive mode places primacy on backing up the data. In its recovery mode, on the other hand, backup processes must either enable the recreation of full operational systems with the latest data or work in conjunction with orchestration platforms to deploy data wherever it is needed.

Business data created by employees on laptops and mobile devices that is stored independently of a sanctioned business system will be ignored in backup processes if these endpoints are excluded.

REPORT CARD FOR RESILIENT DATA BACKUP (ADDITIVE)

Grade	Indicators
Baseline	All data is backed up using multiple storage methods, enabling restoration of any system or application. Restoration procedures are regularly tested and confirmed
Better	Ransomware protections are integrated in backup and restoration procedures
Best	Changing backup settings or deleting backup data is subject to elevated protections

Source: Osterman Research (2022)

6. Prepare to Recover After an Incident

While it is almost certain that every organization will face opportunistic attackers—and perhaps determined ones, too—it is not certain that every organization will become a victim of a ransomware incident. But if that does happen, having a response protocol or recovery plan approved by the Board and ready to enact is invaluable.

STEPS FOR RECOVERING AFTER AN INCIDENT

Essential steps for preparing to recover after compromise are:

- **Develop a recovery plan**
  If your organization suffered a ransomware incident, how would you recover? The extent and impact of a possible incident could range across multiple dimensions, hence plan for several compromise scenarios involving both users and devices, local and remote. Developing a recovery plan before an incident offers two benefits: first, developing a plan doesn't have to be undertaken during the heat of a real incident, and second, identifying weaknesses in current protections enables earlier mitigation.
- **Check and confirm the "small" but critical details**
  Assess, test, and verify that the specifics are appropriate to the risk. If backups are essential for data restoration without paying the ransom, confirm the right backup media is being used and that advanced controls over backup settings have been activated (not merely licensed). If biometric identity controls are being introduced, ensure they are stored securely and subject to the right protections. These and other small details form the foundation for effective and prompt recovery following an incident.
- **Verify insurance coverage is fit-for-purpose**
  Cybersecurity coverage was a goldmine for insurance companies until ransomware payouts severely undermined profitability. Insurance companies offer different types of policies, and untested reliance on the wrong type has costly implications after a ransomware incident. An Australian company recently lost a court case against its insurance provider after claiming for financial damages from a ransomware incident under a traditional crime policy. The company had not taken out insurance coverage specifically for cybersecurity incidents.[22]
- **Reduce the negligence scope**
  Locate and review previous cybersecurity readiness assessments undertaken specifically for your organization. Ensure identified weaknesses have been addressed or mitigated—otherwise a ransomware compromise through any of these will reek of internal negligence. If more than 12 months has elapsed since the last readiness review, commission an update.

If your organization suffers a ransomware incident, what is your response protocol?

REPORT CARD FOR RECOVERING AFTER AN INCIDENT (ADDITIVE)

Grade	Indicators
Baseline	Recovery plan developed, tested, and reviewed regularly
Better	Test and confirm the details on which recovery is built
Best	Conduct regular ransomware readiness assessments and act promptly on the recommendations, including for previous assessments

Source: Osterman Research (2022)

7. Prevent Abuse of Exfiltrated Data

Ransomware attacks are increasingly focused on exfiltrating data rather than encrypting data only, because exfiltrated data adds weight to the extortion used by threat actors against victim organizations when demanding a ransom payment. For example, threat actors tie the ransom payment to preventing the publication, sale, auctioning, or other usage of the stolen data—not for providing the decryption key. While organizations with resilient data backups can overcome operational disruption and avoid paying the ransom to gain a decryption key, and organizations with anti-data exfiltration and DNS monitoring solutions can stop data exfiltration in process, recovering from the theft of readable data is much more difficult. The only viable way to protect organizational data is through pre-exfiltration protection.

SOLUTIONS FOR PREVENTING EXPLOITATION OF EXFILTRATED DATA

Several core data disciplines need greater attention by organizations to prevent exfiltrated data from being exploited. For example:

- **Extend data discovery and data classification beyond sanctioned tools and cloud apps**
  Documents, email messages, and chat threads in unstructured communication and collaboration tools and cloud apps (e.g., Box, Dropbox, OneDrive, SharePoint, Teams, and Google Workspace) are routinely used by employees to exchange information about patients, customers, financial matters, and project details. In addition, cloud apps are being adopted by business units, teams, and individuals to circumvent legacy and restrictive sanctioned apps, creating data repositories that are not as well-protected as those under the purview of IT and security teams. Data discovery and data classification tools enable the identification of confidential, sensitive, and personal data that needs to be protected—irrespective of where that data is stored. Organizations that don't have the visibility and optics into where their data resides cannot protect it.
- **Encrypt data—in-transit, at-rest, and in-use**
  The use of strong data encryption (i.e., stronger ciphers)—intentionally and under the control of the organization—assures data is safeguarded throughout its lifecycle, even if stolen by a threat actor. Encryption solutions are frequently, but not ubiquitously, used with data in-transit and data at-rest. Encryption is less frequently used with data in-use, for example, homomorphic encryption for secure computation. Most organizations have room for improvement in the use of encryption to secure their own data and prevent its exploitation if it is exfiltrated by a threat actor. Encryption and pseudonymization are two data protection technologies mentioned explicitly in the GDPR (General Data Protection Regulation) in the European Union as means of protecting personal data, and reducing the likelihood that a data breach can successfully compromise plaintext data values.

Recovering after the theft of readable data is much more difficult than recovering from malicious data encryption alone.

REPORT CARD FOR PREVENTING ABUSE OF EXFILTRATED DATA (MATURITY)

Grade	Indicators
Low	Sensitive, confidential, personal, and other regulated data is protected at rest and in transit
Medium	All data is protected at rest and in transit
High	All data is encrypted all the time, even during use

Source: Osterman Research (2022)

8. Develop Resilient Operating Processes

Ransomware attacks disrupt normal operating processes. Employees cannot rely on IT systems to accomplish their tasks in the normal way. In some industries, employees may be able to cease operations for several hours without causing significant loss. In other industries, every minute counts—such as healthcare, transportation/logistics, and law enforcement. Leaving it up to staff to scramble and improvise after a ransomware incident is a recipe for costly implications downstream.

SOLUTIONS FOR RESILIENT OPERATING PROCESSES

Developing resilient operating processes includes:

- **Having alternative operating processes on standby**
  Since IT systems will be inoperable after an incident, access to forms and manuals through alternative means will be required. For organizations where it matters, create commonly used forms and manuals for paper-based processes when IT processes are rendered inoperable. Offer staff training on a suitable cadence covering how to access and use these resources. Options include use of the organization's multi-functional printing devices, agreements with local print shops, or USB thumb drives stored securely for use with new printers purchased under urgency after an incident.
- **Preparing to capture data created on paper-based forms**
  For organizations where it matters, data entered on paper-based forms during a ransomware incident, such as patient charts in a hospital, must be accounted for once normal IT systems are restored. Options for capturing data include scanning forms to be associated with a case, project, or patient, automatic conversion techniques to transform handwritten text into machine-readable text, human transcription of captured records, or submission of a photo of a form via a mobile app. Having traceability of actions, decisions, and authorizations during the use of alternative processes is just as important as when normal IT systems are in use. In some industries, not having all records available would be a violation of compliance requirements. In others, it could also be the basis for a disgruntled client or family member to sue for malpractice or negligence.
- **Maintaining back up methods for contacting staff and coordinating with clients**
  Scheduling systems are used for staff rosters, patient bookings, client meetings, raw material movements, and much more. If these systems are compromised through a ransomware incident, lists of upcoming events, and contact details for people will be inaccessible. Even the ability to call people to reschedule meetings or appointments—or recommend other suppliers—will be hampered for as long as systems are out of action, magnifying the chaos across the victim's ecosystem. Options include priority restoration of scheduling systems, regular exports of upcoming events and contact details to a secondary storage system, or integration with air gapped devices receiving regular updates.

Leaving it up to staff to scramble and improvise after a ransomware incident is not ideal.

REPORT CARD FOR RESILIENT OPERATING PROCESSES (ADDITIVE)

Grade	Indicators
Baseline	Alternative operating processes developed, including required forms and manuals. Employees trained on how to work through significant system disruption
Better	Close the loop for data developed/captured using manual processes
Best	Minimize the scope for wider chaos by ensuring staff and clients can be contacted

Source: Osterman Research (2022)

Conclusion

We have examined eight areas for organizations to strengthen in anticipation of further ransomware attacks and incidents. Although attack indicators in 2022 have been lower than expected—due to sanctions against Russia following the invasion of Ukraine—ransomware gangs are extending their crime models, toolkits, and playbooks to inflict significant future damage. Strengthening protections and addressing current weaknesses across these eight areas puts organizations in a much stronger position when ransomware attacks increase again. In addition to reducing the likelihood of compromise at a given organization specifically, elevated protections also decrease the attractiveness and profitability of the ransomware crime model in general.

Strengthen protections and address current weaknesses to reduce the likelihood of compromise and decrease the attractiveness of the ransomware crime model.

Sponsors of this White Paper

ASIGRA

Asigra is the world's most secure data protection platform providing the ultra-secure backup required to fight today's advanced ransomware. With over 20 years of experience protecting the world's largest organizations' data, Asigra takes an entirely different approach to backup security. Asigra provides a truly agentless solution designed to hunt and terminate the advanced attacks targeting backups.

Because immutable and air-gapped backups are routinely infiltrated by ransomware 3.0, Asigra utilizes a multilayered proactive approach, which integrates the industry's #1 ranked anti-ransomware, Content Disarm and Reconstruction (CDR), Deep MFA, FIPS 140-2 encryption, and more. Asigra is a three-time winner of Product of the Year from TechTarget for Enterprise Backup Software.

More information on Asigra can be found at www.asigra.com.

www.asigra.com

info@asigra.com

@asigra

+1 877 736 9901

BLACKFOG, INC.

Founded in 2015, BlackFog is a global cybersecurity company that has pioneered on-device Anti Data Exfiltration (ADX) technology to protect companies from global security threats such as ransomware, spyware, malware, phishing, unauthorized data collection, and profiling. Its software monitors enterprise compliance with global privacy regulations and prevents cyberattacks across all endpoints. BlackFog uses behavioral analysis to preemptively prevent hackers from exploiting vulnerabilities in enterprise security systems and data structures.

BlackFog's preventative approach to security recognizes the limitations of existing perimeter defense techniques and neutralizes attacks before they happen at multiple points in their lifecycle. Trusted by corporations all over the world, BlackFog is redefining modern cybersecurity practices.

Visit www.blackfog.com.

www.blackfog.com

info@blackfog.com

@blackfogprivacy

CYREN

Cyren protects more than a billion users around the world from sophisticated and emerging email, malware, and web cyber-attacks every day. Our embedded threat detection, threat intelligence and inbox security solutions help enterprises, service providers, and technology companies prevent breaches and eliminate countless hours of incident response.

Phishing and Business Email Compromise
Cyren Inbox Security eliminates the time your security teams spend manually hunting and removing email threats.

Malware Detection and Analysis
Cyren provides multiple, embedded malware detection and analysis solutions to block known and unknown ransomware threats without compromising performance or privacy.

Learn more at www.cyren.com.

www.cyren.com

@CyrenInc

info@cyren.com

+1 703 760 3320

INFOBLOX, INC.

Infoblox is the leader in next-generation DNS management and security. Our core network services expertise enables us to apply unique ML/AI analysis at the DNS level to identify and block threat activity most defenses cannot see, while expandable and customizable threat intelligence speeds incident investigation and accelerates threat resolution.

Additional options include a massive ecosystem of partners and integration capabilities to uplift capabilities across the entire security stack through automated threat intel collection and distribution, event data sharing, and incident response actions to uplift the ROI for all security investments. Infoblox provides our customers, including 70% of the Fortune 500, with the security visibility, control, and automation they need to address the challenges of the hybrid workplace that often includes IoT, BYOD, ICS and more.

Learn more at www.infoblox.com.

www.infoblox.com

info@infoblox.com

+1 408 986 4000

IRONSCALES

IRONSCALES is a leading email security company focused on fighting back against today's modern phishing attacks. Our self-learning, AI-driven platform continuously detects and remediates advanced threats like Business Email Compromise (BEC), credential harvesting, Account Takeover (ATO) and more. We believe our powerfully simple email security solution is fast to deploy and easy to manage and keeps our customers safe.

Founded in Tel Aviv, Israel in 2014 by alumni of the Israel Defense Force's elite Intelligence Technology unit, IRONSCALES is headquartered in Atlanta, Georgia. We are proud to support thousands of customers globally with our award-winning, analyst-recognized platform.

Visit www.ironscales.com to learn more.

www.ironscales.com

@IRONSCALES

MICRO FOCUS

Micro Focus is one of the world's largest enterprise software providers, focused on solving the IT dilemma—how to balance today's needs with tomorrow's opportunities. We deliver mission-critical technology that helps tens of thousands of customers worldwide manage core IT elements of their business. Strengthened by our strategic services and support organizations, and an extensive partner network, our broad set of technologies for security, IT operations, application delivery, governance, modernization, and analytics provides the innovative solutions organizations need to run and transform— at the same time. The Information Management & Governance Product Group delivers core solutions every business needs to manage, protect, and secure their data, while enabling effective collaboration, from anywhere, on any device. The difference is that we focus on the power of strategic insight to know your data, empower your people, and drive your future.

Visit www.microfocus.com.

www.microfocus.com

@MicroFocus

+1 877 686 9637

SONICWALL

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide.

For more information, visit www.sonicwall.com.

www.sonicwall.com

@SonicWall

+1 888 557 6642

TREND MICRO

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints.

The Trend Micro One unified cybersecurity platform delivers advanced threat defense techniques, extended detection and response (XDR), and integration across the IT ecosystem, including AWS, Microsoft, and Google, enabling organizations to better understand, communicate, and mitigate cyber risk.

With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world.

Visit www.trendmicro.com.

www.trendmicro.com

@TrendMicro

+1 888 762 8736

[1] Sergiu Gatlan, Lincoln College to close after 157 years due ransomware attack, May 2022, at https://www.bleepingcomputer.com/news/security/lincoln-college-to-close-after-157-years-due-ransomware-attack/
[2] Howard Blume, Criminal syndicate claims credit for LAUSD hack; authorities won't say whether it's true, Los Angeles Times, September 2022, at https://www.latimes.com/california/story/2022-09-09/criminal-syndicate-claims-credit-for-lausd-hack-says-it-holds-sensitive-information
[3] Douglas Jose Pereira dos Santos, Key Findings from the 1H 2022 FortiGuard Labs Threat Report, August 2022, at https://www.fortinet.com/blog/threat-research/fortiguard-labs-threat-report-key-findings
[4] Danny Palmer, This company was hit with ransomware, but didn't have to pay up. Here's how they did it, December 2021, at https://www.zdnet.com/article/this-company-was-hit-with-ransomware-but-didnt-have-to-pay-up-heres-how-they-did-it/
[5] Stephanie Kelly and Jessica Resnick-Ault, One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators, June 2021, at https://www.itnews.com.au/news/one-password-allowed-hackers-to-disrupt-colonial-pipeline-ceo-tells-senators-565671
[6] Infoblox, 2022 Global State of Security Report: Remote Workers Spell Trouble for InfoSec, June 2022, at https://info.infoblox.com/resources-whitepapers-new-cyberrisk-alliance-and-infoblox-report-remote-workers-spell-trouble-for-infosec
[7] BlackFog, BlackFog Global Ransomware Report - August 2022, September 2022, at https://privacy.blackfog.com/wp-content/uploads/2022/09/BlackFogRansomwareReport-Aug-2022.pdf
[8] BlackFog, BlackFog Global Ransomware Report - September 2022, October 2022, at https://privacy.blackfog.com/wp-content/uploads/2022/10/BlackFogRansomwareReport-Sep-2022.pdf
[9] BlackFog, BlackFog Global Ransomware Report - July 2022, August 2022, at https://privacy.blackfog.com/wp-content/uploads/2022/08/BlackFogRansomwareReport-Jul-2022.pdf
[10] Trend Micro, 2022 Midyear Cybersecurity Report: Defending the Expanding Attack Surface, August 2022, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/defending-the-expanding-attack-surface-trend-micro-2022-midyear-cybersecurity-report
[11] European Union Agency for Cybersecurity, Hackers-for-Hire drive the Evolution of the New ENISA Threat Landscape, October 2021, at https://www.enisa.europa.eu/news/enisa-news/hackers-for-hire-drive-the-evolution-of-the-new-enisa-threat-landscape
[12] SonicWall, 2022 SonicWall Cyber Threat Report: Mid-Year Update, July 2022, at https://www.sonicwall.com/2022-cyber-threat-report/
[13] KELA Cybercrime Prevention, Ransomware Victims and Network Access Sales in Q2 2022, August 2022, at https://ke-la.com/wp-content/uploads/2022/08/KELA-RESEARCH_Ransomware-Victims-and-Network-Access-Sales_Q2-2022.pdf
[14] David Claridge, Are Sanctions the Answer in Ransomware Prevention?, Geopolitical Monitor, August 2022, at https://www.geopoliticalmonitor.com/are-sanctions-the-answer-in-ransomware-prevention/
[15] BlackFog, BlackFog Global Ransomware Report - August 2022, September 2022, at https://privacy.blackfog.com/wp-content/uploads/2022/09/BlackFogRansomwareReport-Aug-2022.pdf
[16] WatchGuard, Internet Security Report - Q1 2022, June 2022, at https://www.watchguard.com/wgrd-resource-center/security-report-q1-2022
[17] Corvus Insurance, How to Prepare for a Cyber Hurricane: 3 Key Takeaways, May 2022, at https://www.corvusinsurance.com/blog/how-to-prepare-for-a-cyber-hurricane-3-key-takeaways
[18] KELA Cybercrime Prevention, Ransomware Victims and Network Access Sales in Q2 2022, August 2022, at https://ke-la.com/wp-content/uploads/2022/08/KELA-RESEARCH_Ransomware-Victims-and-Network-Access-Sales_Q2-2022.pdf
[19] Jessica Lyons Hardcastle, Uber explains how it was pwned this month, points finger at Lapsus$ gang, September 2022, at https://www.theregister.com/2022/09/19/uber_admits_breach/
[20] Veeam, 2022 Ransomware Trends Report, June 2022, at https://go.veeam.com/wp-ransomware-trends-report-2022
[21] Chris Hoff, Ransomware: Secure Backup Is Your Last Line of Defense, April 2022, at https://www.veeam.com/blog/secure-backup-ransomware-defense.html
[22] Lockton, Cyber in Focus: what boardrooms need to know, August 2022, at https://global.lockton.com/au/en/news-insights/cyber-in-focus-what-boardrooms-need-to-know