Acronis

WHITE PAPER

A 12-step cyber resilience plan for business

Integrate defense and recovery to minimize downtime and data loss

Cyberthreats are growing, led by ransomware and abetted by AI

Ransomware remains the malware tool of choice for cybercriminals to enrich themselves by threatening businesses with data loss, downtime and deliberate leaking of sensitive data. According to the Acronis Cyberthreats Report, H1 2024, ransomware increased 23% in Q1 2024 over Q1 2023.

The latest surge has ballooned the average cost of a data breach from $4.55 million per incident in 2023 to $5.53 million in 2024, according to IBM's Cost of a Data Breach 2024 report. The advent of generative artificial intelligence (GenAI) tools like ChatGPT has further improved the effectiveness and scale of ransomware attacks and made it easier for low-skilled criminals to get into the game.

Attack tactics have also evolved. Encryption of a target's critical data is no longer the sole method to extract ransoms. Most ransomware attackers now precede the encryption stage by first stealing sensitive data so they can threaten to leak it online if the target fails to pay the ransom. Attackers may also contact the target's customers and partners with the threat that their private data may also be leaked, adding pressure to comply with the extortion demand.

Criminals are using ChatGPT and similar tools to improve the apparent authenticity and trustworthiness of phishing emails, to automatically scan applications for vulnerabilities, and to improve the orchestration of multistage attacks.

Spiraling cybercrime has changed the compliance, standards and insurance landscape

AI-enabled improvements to cyberattacks, extortion tactics and attack frequency have increased the pressure on businesses to improve their cyber resilience from three directions: regulatory authorities, cybersecurity standards developers and the insurance industry. Consider:

- **Forthcoming new compliance standards** like the European Union (EU) Digital Operational Resilience Act (DORA), as well as revisions to existing compliance standards like the EU's Network and Information Systems Directive 2022/0383 (NIS 2).
- **New versions of existing cybersecurity standards** like the USA National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Version 2.0, a/k/a/ NIST CSF 2.0.
- **Evolving insurability standards** for businesses to qualify for cyber insurance policies.

[1] Acronis, "Acronis Cyberthreats Report, H1 2024." https://www.acronis.com/en-us/resource-center/resource/acronis-cyberthreats-report-h1-2024/
[2] IBM, "Cost of a Data Breach Report 2024." https://www.ibm.com/reports/data-breach

In each of these cases, the regulations, standards and qualification rules have evolved to add new requirements for cybersecurity defensive measures. For example, requirements to deploy endpoint anti-malware and multifactor authentication have been expanded to include newer technologies like endpoint detection and response (EDR). At the same time, regulators, standards bodies and insurers are now recommending or requiring the deployment of new recovery measures that can quickly restore a business's uptime and data integrity when an incident inevitably does occur. For example, in addition to having robust backup technology and procedures, business are now expected to have disaster recovery and incident response plans in place.

Cyber resilience reduces business risk on many fronts

These expanded requirements for both defense and recovery reflect a recognition that in a world of booming cybercrime abetted by GenAI tools, cybercriminals are going to regularly succeed in their attacks. The new requirements also address other common sources of data loss and downtime, like employee error, software flaws, IT hardware failures and climate disasters. A well-designed cyber resilience regimen demands that businesses become equally adept at fending off incidents where they can and recovering briskly from them when their defenses fail.

A 12-step cyber resilience plan for business

To build this kind of cyber resilience, Acronis recommends the adoption of the following 12-step plan to counter AI-enabled ransomware and other threats, which yields the added benefit of improving a business's ability to recover from other sources of downtime and data loss like human error. This white paper groups these tactics into three categories: defensive measures, skills and processes for IT and cybersecurity operations, and recovery measures.

Defensive measures

1. Deploy AI-enabled anti-malware on endpoints and EDR across the business

To keep up with the flood of GenAI-sharpened attacks, businesses must deploy anti-malware measures that are similarly empowered with machine learning and AI to adaptively identify threats by their behavior. EDR has also become an essential countermeasure to defeat more sophisticated attacks that employ reconnaissance, persistence, privilege escalation, living-off-the-land tactics and lateral movement.

EDR enables defenders to correlate potential indicators of compromise (IOCs) more effectively across multiple endpoints, swiftly contain attacks, investigate incidents to identify any vulnerabilities that allowed the attack, and remediate those weaknesses against future attacks.

2. Update countermeasures like email security and URL filtering

Email remains the most effective vector for cyberattacks: Fully 27.6% of all received emails are spam and 1.5% contain malware or phishing links, per the Acronis Cyberthreats Report, H1 2024. The number of email attacks detected in H1 2024 surged by 293% compared to the first half of 2023, while 26% of users encountered phishing attempts through malicious URLs.

In response, one of the most effective acts of triage a business can perform is investing in up-to-date email security that detects and filters out phishing emails before they hit the employee inbox, and blocks access to malicious URLs before unsuspecting users can click on them.

3. Deploy tools that increase your visibility of IT resources and data flows

A typical question from management to IT following a ransomware attack is, "How did an attacker exfiltrate a terabyte of our sensitive data without us knowing?" To help avoid this painful moment, businesses should instrument their IT infrastructure to monitor and log internal activity (including access to cloud services) and conduct ongoing log analysis.

IT inventorying and data loss prevention (DLP) tools can also provide better visibility to normal vs. anomalous patterns of data storage and movement to detect suspicious activity and lock down potential exposures. This is another area where EDR's real-time monitoring and correlation of IOCs can help.

4. Eliminate external and internal network exposures

Network vulnerabilities are another common attack vector. Businesses should take basic measures like disabling Microsoft Remote Desktop Protocol (RDP) except where it is necessary, and otherwise hardening endpoints by disabling unused services. Other basic steps include:

- **Deploy firewalls** and intrusion prevention systems to limit inbound internet access.
- **Consider limiting VPN access** to specific geographic locations and establishing a remote-work policy that limits or prohibits access to company resources from personal devices.
- **Segment internal networks** to thwart the propagation of ransomware from compromised systems to other endpoints and servers.

5. Manage passwords and access rights vigilantly

Leaked or stolen credentials contributed to 24% of all reported breaches, and credentials are compromised in 50% of all phishing attacks, according to the Verizon 2024 Data Breach Investigations Report. Ransomware attackers commonly exploit passwords that have been

leaked, are reused across multiple accounts, do not meet entropy recommendations, and use only single-factor authentication. Attackers often commandeer IT operations tools like Mimikatz to steal passwords stored in memory on servers.

To combat these tactics, businesses should implement multifactor authentication, especially on systems with sensitive data. Other steps include:

- **Always change administrative login** credentials from their factory default settings.
- **Change all passwords** after a successful attack, as cybercriminals are known to re-attack a prior target using the same compromised credentials that enabled the first attack.
- **Adopt the principle** of least privilege for access rights.
- **Tightly control access** to systems with powerful administrative tools or sensitive data, excluding all but essential employees.
- **Make privileges** time limited or one time only, where possible.

IT and cybersecurity skills and processes

6. Build a security awareness training program

Phishing remains the most effective technique for getting malware inside a company's external defenses, so reducing the number of clicks on malicious attachments and links in emails (as well as in SMS, instant messaging and social media apps) can yield significant risk reductions. Train users to keep their antennae up for suspicious communications by routinely sending them fake phishing emails; offer refresher courses to those who fall for the ruse. Make sure every employee participates, including and especially senior executives, as they are favorite targets due to their elevated privileges and ability to authorize money transfers.

7. Implement automated, programmatic vulnerability scanning and patch management

The typical business struggles to install software patches from its tech vendors in a timely fashion, leaving vulnerabilities unpatched for over 88 days on average. Cybercriminals are aware of these exposures and constantly probe for them. To close these gaps quickly and efficiently, businesses should deploy automated vulnerability scanning and patch management tools to improve the efficiency and accuracy of this tedious but critical IT operations chore.

8. Reduce the number of agents on endpoints and consoles in your operations center

The typical business has deployed its cybersecurity and data protection solutions in piecemeal fashion over time, resulting in a proliferation of remote agents on endpoints and management consoles at the IT operations desk. Multiple endpoint agents waste resources and often conflict with each other. Swiveling between consoles reduces IT operational efficiency and increases training costs.

Businesses should consolidate agents wherever possible to eliminate gaps and conflicts and to improve endpoint performance. Combining management console functionality wherever possible will help to maximize the effectiveness and minimize the onboarding time of IT personnel.

[3] Verizon, "2024 Data Breach Investigations Report." https://www.verizon.com/business/resources/reports/dbir/

9. Take advantage of security frameworks like NIST to regularly assess and update defense and recovery strategies for ransomware attacks and other incidents

Businesses should take advantage of popular (and free to use) cybersecurity frameworks like the NIST CSF, ISO/IEC 27000 family, and CIS Critical Security Controls. These frameworks offer proven best practices and guidance to help businesses prioritize their investments in defense and recovery, and to continuously improve their technology, processes and people skills.

Recovery measures

10. Implement a robust data protection regimen

Attackers always have a first-mover advantage, and even the best-designed defenses can fail to defeat new tactics and technology. Businesses must start from the assumption that an attack will succeed at some point and strive to improve their data protection regimen as a last line of defense. Restoring data from a recent backup may enable the quick resumption of business operations without paying a ransom.

However, note that attackers often attempt to locate and encrypt or delete backup archives, disable backup and security measures, and use the target's own cybersecurity, IT operations and backup tools to steal data and move laterally across the internal network. Thus, businesses should:

- **Keep multiple encrypted copies** of backups on different media and in separate locations (off-site, offline, and in the cloud).
- **Conduct regular live tests** of their backup plan to validate the integrity of backup archives and processes.
- **Use testing to validate** that restoral can be executed swiftly enough to meet the business's recovery time objectives.
- **Scan backups for malware** and unpatched vulnerabilities and remediate those issues before restoring systems and putting them back into production.
- **Implement immutable storage** of backup archives to thwart backup deletion tactics.

11. Consider implementing a disaster recovery program

The process of cleanup and recovery after a downtime or data loss incident, including the restoral of large amounts of data from backup, can postpone the resumption of normal business operations by days or weeks. Businesses should thus consider deploying disaster recovery services that enable immediate resumption of operations using replicated applications and data (either off-site or in the cloud). Cloud-based disaster recovery services have made this contingency much more affordable and simpler to manage — even for smaller businesses.

12. Build an incident response plan and regularly test and update it

Every business should have an incident response plan (IRP) with the following essential components:

- **A list of the names and numbers** of essential internal and external contacts in hard copy form, as a ransomware attack may make online records inaccessible.
- **A reliable fallback** internal communications channel (e.g., a smartphone messaging or social media app) in the event that systems like email become inoperable.
- **A documented communications plan** that identifies which audiences need to be informed, and by whom, based on the severity and stage of the attack:
  - IT and security operations and management, executive leadership, legal and compliance teams, partners and customers, the press and the public, regulatory authorities, bankers and investors, etc.

Businesses should evaluate their plan regularly with both tabletop and live exercises at least once a year, and always immediately after an incident. The plan should include measures to collect forensic data that can be used after an incident to identify the vulnerabilities that enabled the breach, remediate them and update the response plan accordingly.

Conclusion

Any business that hopes to reduce its risk from the growing threat of AI-enabled ransomware and other threats to data integrity and uptime must get aggressive on defense, but also plan for the probability that an attack will succeed.

To counter the growing sophistication and frequency of these incidents, business leaders must focus their defense and recovery planning on processes and technology that reduce overall complexity and strengthen their IT staffers with the use of AI, automation and integration. In addition to reducing overall business risk, these investments will also improve a business's ability to meet regulatory compliance requirements, align with industry best practices articulated by cybersecurity frameworks, and qualify for competitively priced cyber insurance.

Further reading

↘ Acronis Cyberthreats Report, H1 2024.

↘ White paper: Is your business ready for NIS 2 compliance?

↘ White paper: Business continuity: Shifting from passive planning to active risk mitigation.

↘ Infographic: Top 5 reasons your business needs to be protected with EDR right now.

↘ Acronis blog: Murphy's Law and the lessons of the CrowdStrike outage.

↘ Acronis blog: Keep your business current with evolving IT compliance requirements.

↘ Acronis blog: Lessons learned from the UnitedHealthcare cyberattack.

Talk to an expert

To get a complimentary consultation with an Acronis solutions engineer to explore how your business can improve its cyber resilience, contact Acronis here.

Get a complimentary 30-day trial of Acronis Cyber Protect here.

About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs) and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect Cloud is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses. Learn more at www.acronis.com.

Acronis

Learn more at
www.acronis.com