SENTIS
Managed Solutions

2023 Ransomware Survival Guide

Ransomware and its associated attack vectors are on a staggering upward trajectory. And there's one sector in particular that threat actors relentlessly target – professional services.

This guide provides strategical and operational insight to help you survive the ransomware epidemic, and protect your data, operations and bottom line.

Trending Ransomware Risk Markers

How is ransomware risk worsening and which of its related tactics should professional services be best prepared for? Here are your professional services-specific need-to-know statistics.

243% increase in ransomware attacks (1)

Ransomware attacks are rising in professional services, despite falling for businesses overall. Cyber insurance is credited with the broader decrease because policies can't be underwritten without specific security measures in place. Is cyber insurance under-utilised in professional services? It may be worthwhile checking the products available.

269% increase in cryptojacking (2)

Cryptojacking is a lower-risk method of extorting money because it's "quieter" than traditional ransomware attacks, which rely heavily on social engineering like phishing emails. Threat actors are tempted by the low-risk, high-payoff promise of cryptojacking attacks, which explains its astronomical surge in their professional services.

152% increase in encrypted attacks(3)

As advanced persistent threats – where sophisticated ransomware sits in and surveils IT infrastructure over several weeks or months – increase, it's no surprise that encrypted attacks are on the rise too. Long dwell times give threat actors time to decrypt data, and re-encrypt with their codes – effectively ransoming all data, even backups.

151% increase in IoT malware (4)

As professional services organisations digitally mature to meet customer and regulatory demand, IoT technology follows. Although delivering huge advantages in areas like fraud detection, auditing speed and customer service, unprotected IoT technology expands attack surfaces for ransomware infection.

45% increase in never-before-seen malware (5)

Never-before-seen describes malicious activity not previously identified by anti-malware software or threat intelligence parties. This is often a precursor to day-zero attacks, which are both unidentified and target unprotected vulnerabilities, such as unpatched systems. The most devasting malware has these characteristics.

44% increase in intrusion attempts (6)

An intrusion attempt occurs when a threat actor attempts to gain unauthorised access to systems or resources by exploiting a weakness. This can be executed by external threat actors, or malicious insiders. Given the vast amount of financial, regulated and operational-critical data stored in professional services systems, these attacks can be costly.

Professional Services Cybersecurity Investment Priorities

Where are professional services IT and business leaders investing to manage, mitigate and minimise ransomware risk and attack damages?

Zero-trust permissions adoption

Artificial Intelligence **threat detection**

Cyber insurance underwriting

RegTech compliance software

Anti-Ransomware Quick Wins

1. Update and patch operating systems and apps
2. Disable inactive user accounts and devices
3. Set up and cycle strong passwords
4. Implement password multi-factor authentication
5. Apply least-privileged access permissions
6. Implement PDNS and DMARC email security
7. Check cloud or on-premises backups are working
8. Arrange user security awareness training
9. Deploy endpoint detection and response (EDR)

Do you need any help specifying what the above terms mean and how they affect your organisational resiliency and security posture? Get in touch with Sentis Managed Solutions on **0345 862 2930** to ask your questions. Our advice is no-obligation.

w: sentisms.com **t: 0345 862 2930** **e: itaudit@sentisms.com**

Strategic Anti-Ransomware Checklist

The best way to combat ransomware is to build a layered security stack where functions interlink to cover every corner of IT infrastructure. This approach enables organisations to eliminate blind spots and weak points, and effectively contain and isolate active threats to reduce damage and ensure business continuity.

These are the **eight layers of a resilient security stack** that will help manage, mitigate and minimise your ransomware risk.

LAYER **1**	**Critical Operations**	☐ Secure hosting – on-premises and cloud ☐ Disaster recovery process and failovers
LAYER **2**	**Data Security**	☐ Encryption in rest and transit ☐ Immutable cloud backups ☐ Permissions and governance management
LAYER **3**	**Application Security**	☐ Patch management ☐ Vulnerability scanning ☐ Application whitelisting
LAYER **4**	**Endpoint Security**	☐ Endpoint Detection and Response ☐ Multifactor authentication
LAYER **5**	**Network Security**	☐ Next Generation Firewall ☐ Network segmentation ☐ VPN ☐ Network Detection and Response ☐ Web content filtering
LAYER **6**	**Perimeter Security**	☐ Patch management ☐ Email security and filtering ☐ Advanced Threat Protection (AV) ☐ Security Information and Event Monitoring ☐ Security Operations Centre
LAYER **7**	**The Human Element**	☐ Security Awareness training ☐ Threat simulation testing ☐ Identity management solutions
LAYER **8**	**Evolving Your Environment**	☐ IT infrastructure audit ☐ Digital transformation roadmap ☐ Policy and compliance management

To find out what the above solutions protect against, how they work together and why aiming for a layered stack is important, get in touch with Sentis Managed Solutions. Call us on **0345 862 2930** to arrange a no-obligation consultation or read about our Secure by Sentis products at **sentisms.com/security/**

w: sentisms.com **t: 0345 862 2930** **e: itaudit@sentisms.com**

What to Look for in a Security Audit

What does our audit do?

We analyse your entire IT environment to uncover critical risks, and pinpoint where technology can **work harder and smarter** in your business. This vital service is entirely free when provided by Sentis Managed Solutions and audits everything you see here as standard.

What happens afterwards?

We review our findings in a **comprehensive, clear-cut report.** We also make **tailored recommendations** for improvements, focused on
1) achieving IT best practice
2) reducing critical risks
3) data and systems protection in the event of a disaster

How do we measure risk?

To clarify our findings and help you prioritise, a straightforward Red, Amber, or Green rating is applied to each element audited.

Critical Risk

Improvement Required

Good Standard

CORE INFRASTRUCTURE	Servers, inc. hardware, OS, environment and physical security. Network switch hardware. Structured cabling.
DATA SECURITY MANAGEMENT	Password management, inc. multifactor authentication and admin rights. Policies, inc. group, BYOD, data storage and GDPR. Staff awareness training & testing.
DATA SECURITY SOFTWARE	Perimeter software, inc. firewalls, antimalware. Email and web content filtering. Security patch management and endpoint encryption.
DISASTER RECOVERY	Network and server break/fix cover. DR application or cloud solution with RPO and RTO. Document procedures.
SUPPORT	Helpdesk, change, asset and capacity management.
ENDPOINTS	Laptop and PC hardware, operating systems and printers.
NETWORKING	Wireless networking, telephony, Internet and IP configuration.
APPLICATIONS	Office, Exchange, M365, and storing sensitive data effectively in the cloud.

w: sentisms.com **t: 0345 862 2930** **e: itaudit@sentisms.com**

Ransomware Survival Glossary

A

Advanced Persistent Threat (APT):

Targeted, sophisticated cyberattacks that employ multiple attack vectors and techniques over an extended period, typically aimed at high-value assets or organisations.

Advanced Threat Protection (ATP):

A comprehensive cybersecurity solution that detects, prevents, and responds to advanced threats, including malware, ransomware, APTs, and other sophisticated attacks, using multiple security layers and threat intelligence.

C

Cryptojacking:

The unauthorised use of an endpoint, application, system or network to mine cryptocurrency, typically achieved by installing malware that uses the computer's processing power without the owner's consent.

Cyber insurance:

A type of insurance that provides financial protection to organisations and individuals in the event of a cyberattack or data breach, covering losses and liabilities resulting from such incidents.

Cyber fatigue:

A state of weariness or apathy that can occur when people are exposed to a large volume of cybersecurity alerts, warnings, and messages, leading to decreased awareness, vigilance, and responsiveness to cyberthreats.

D

Day-zero attacks:

Zero-day cyberattacks are exploits or vulnerabilities that target software flaws that are unknown to the software vendor or the security community, enabling attackers to infiltrate and compromise a system before a patch or fix is available.

DMARC:

DMARC (Domain-based Message Authentication, Reporting, and Conformance) email security is an email authentication protocol that helps organisations prevent email spoofing, phishing, and other types of email-based fraud by providing a framework for email authentication and reporting.

Decryption:

The process of converting encrypted data back into its original, plaintext form using a decryption key, which reverses the encryption process and makes the data readable and usable.

E

Endpoint Detection and Response (EDR):

A cybersecurity technology that monitors and analyses endpoint activity to detect and respond to advanced threats, providing real-time visibility, threat hunting, and incident response capabilities.

Encrypted attacks:

Cyberattacks that use encryption to conceal malicious traffic or communications, making it difficult for security solutions to detect or inspect the attack traffic and prevent the attack.

I

Immutable Storage Backup (ISB):

A data backup and recovery solution that uses write-once-read-many (WORM) technology to create unalterable backups, providing an extra layer of protection against data tampering or deletion, ransomware attacks, and other cyber threats.

Intrusion attempts:

Unauthorised efforts to access, infiltrate, or compromise a computer system, network, or application, often using various techniques such as scanning, probing, or exploiting vulnerabilities to bypass security measures.

IoT devices:

IoT (Internet of Things) devices are physical objects with embedded sensors, processors, and connectivity that enable them to exchange data with other devices and systems, allowing for remote monitoring, control, and automation.

M

Malicious insiders:

Malicious insiders are authorised individuals, such as employees, contractors, or partners, who intentionally or unintentionally exploit their access to sensitive information or systems to cause harm, steal data, or disrupt operations.

Multifactor authentication:

A security mechanism that requires users to provide two or more forms of authentication, such as a password and a biometric or a security token, to access a system or service.

N

Network Detection and Response (NDR):

A cybersecurity technology that monitors network traffic to detect and respond to advanced threats, providing real-time visibility, threat hunting, and incident response capabilities for network-based attacks.

Network segmentation:

The practice of dividing a network into multiple subnetworks or segments, with restricted access and specific security policies, to reduce the attack surface and limit the impact of a security breach.

Next Generation Firewall (NGFW):

A network security solution that combines traditional firewall capabilities with advanced security features, such as application identification and control, intrusion prevention, and advanced threat protection.

P

PDNS:

PDNS (Passive DNS) email security is a threat intelligence technology that provides visibility into the historical DNS activity of domains and IP addresses associated with email-based threats, allowing for proactive defence against such threats.

R

Ransomware:

A type of malware that encrypts files on a victim's system and demands a ransom payment in exchange for the decryption key, often delivered through anonymous cryptocurrency payments.

Ransomware dwell:

The amount of time that ransomware remains undetected on a victim's system or device before it is identified and remediated, typically measured in days, weeks or months.

RegTech:

RegTech (Regulatory Technology) is the use of technology, such as AI, machine learning, and automation, to help organisations comply with regulatory requirements and manage regulatory risk, reducing manual efforts and improving efficiency.

S

Security Information and Event Monitoring (SIEM):

A cybersecurity technology that collects and analyses security-related data from various sources to provide real-time threat detection, incident response, and compliance management capabilities for organisations.

Security Operations Centre (SOC):

A centralised facility that manages and monitors an organisation's security posture, using advanced technologies and processes to detect, investigate, and respond to security incidents and threats.

Simulation testing:

The practice of creating realistic scenarios, such as phishing attacks or malware infections, to train security personnel and assess their readiness to detect and respond to real-world threats.

Social engineering:

The practice of exploiting human psychology, rather than technical vulnerabilities, to gain access to sensitive information or manipulate individuals into performing certain actions.

T

Threat actor:

Any person, group, or organisation that has the intent and ability to conduct malicious activities against targets, such as launching cyberattacks, stealing sensitive information, or disrupting critical systems.

(1) https://www.continuitycentral.com/index.php/news/technology/7537-sonicwall-threat-report-highlights-significant-changes-in-the-threat-landscape

(2) https://www.coindesk.com/business/2022/07/26/cryptojacking-in-financial-sector-has-risen-269-this-year-sonicwall-says/

(3) https://blog.checkpoint.com/securing-the-cloud/addressing-the-rising-threat-of-web-ddos-tsunami-attacks-in-2023/

(4) https://securitybrief.co.nz/story/global-ransomware-grows-151-sonicwall-research-finds

(5) https://www.sonicwall.com/medialibrary/en/infographic/mid-year-update-2022-sonicwall-cyber-threat-report.pdf

(6) https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf

SENTIS
Managed Solutions

w: sentisms.com t: 0345 862 2930 e: itaudit@sentisms.com