Risky connections:
Ransomware's unique and escalating threats to technology companies

Ransomware table of contents

Gain insight on –

Extortion by ransom is no longer just the purview of kidnappers.

Ransomware is big business for cybercriminals and big trouble for technology and life sciences companies that are targeted.

Kaseya, a leading provider of IT and security management solutions for managed service providers and small to midsized businesses, was attacked by ransomware in July 2021. The attack compromised the company's software, and hundreds of its customers were extorted.[1]

Foxconn, the largest electronics manufacturing company in the world, was attacked in 2020. More than 1,000 servers were encrypted, and more than 100 gigabytes of data was exfiltrated and ransomed for $34 million.[2]

Acer, the large computer company, was hit by a hacking group that demanded $50 million in what was one of the biggest ransomware demands of 2021.[3]

Olympus, a large technology company, was attacked by a group using ransomware as a service (RaaS) tools.[4]

Attackers have developed new ways to find systems that are vulnerable to ransomware and deploy sophisticated scams that dupe the most skilled computer user. Adding to the nature of the threat, artificial intelligence is used to write phishing emails that perform better than those written by people. These attacks disrupt operations and the provision of services, risk the loss of critical information and data, and destroy brands and reputations.[5]

Attackers have developed new ways to find systems that are vulnerable to ransomware

It is more important than ever for technology and life sciences entities to understand the threat ransomware poses and the steps necessary to safeguard their businesses.

(Return to Table of Contents)

Ransomware: An expensive threat to technology businesses.

Ransomware is a type of malware that anyone in your organization can unknowingly download by opening an email attachment, clicking an ad, following a link or visiting a website that is embedded with malware. Often, you will never know your computer or your system has been targeted and infected.

Remediation costs from attacks cost companies an average of $700,000

Once the ransomware code finds a home in your system, it will encrypt files and data, making it impossible to access your computers or use any systems that rely on them. Then the attacker crawls your system, looking for sensitive data (like client information and intellectual property) and backup systems that are then targeted for deletion. The criminals behind the attack then demand a ransom, usually in bitcoin, in exchange for decryption tools and access back into your system. Demands can also include additional pressure for payment via threats of releasing sensitive or confidential data.

As its name suggests, ransomware holds your computer system hostage until payment is made. In 2020, the average ransom payment was over $170,000. But the ransom payment itself is only one part of the total cost of ransomware. From shutdowns and lost revenue to legal fees and remediation costs, these attacks cost companies an average of $700,000.[6]

Because of the increasing sophistication of cybercriminals and their malware, it is becoming much harder for businesses to recover from ransomware attacks. In 2020, ransomware attacks, on average, caused 18 days of downtime for affected companies. A technology business caught unprepared to defend against ransomware can be crippled or even forced to close its doors.

(Return to Table of Contents)

Unique impacts of ransomware on technology and life sciences companies.

Technology companies typically have valuable intellectual property and consumer data that they need to protect, as well as deeper pockets that can support high ransom demands.

Cybercriminals know this and exploit it to their advantage. Current trends are for attackers to also capture sensitive data leading to two ransom demands: one for access to systems and data, and the other for a promise not to publicly release systems, data and intellectual property.

Characteristics of technology companies that deserve special consideration

Electronic Manufacturing:

Automation, digitization and the introduction of the Industrial Internet of Things (IIoT) into the manufacturing process make electronic manufacturing more connected to the internet. This creates security challenges and exposes potential system vulnerabilities that may open doors to cyberattacks such as ransomware. Using overseas third-party suppliers is common in the industry, but risks of a cyberattack increase without regular reviews of these suppliers' security architecture. Plus, end-of-life technology, which no longer receives hardware or software updates or support, can be a cybercriminal's backdoor to security and operating systems. This sort of product obsolescence and lack of support can lead to increased potential for attack. It is important for technology companies to manage end-of-life product support for equipment still in use, whether in their environment or in their customers' environment.

Life Sciences:

System vulnerabilities of life sciences companies coupled with other ineffective cybersecurity practices can make it easy to corrupt or steal important research data, pricing and commercialization details, as well as sensitive patient information. In addition, medical devices, which are increasingly connected to health care system networks, are prone to exploitation, potentially putting patient health at risk. Cybercriminals know that many health care systems lack consistent cybersecurity for their networked medical devices, making these especially easy targets.

IT/Software:

Multiple suppliers and a large remote workforce put technology and software service providers at risk for ransomware. A large remote workforce using their own devices and not surrounded by a corporation's secure network can create an open door for ransomware to penetrate the corporate system. Once the cybercriminals have gained access, software corrupted with malware could then be distributed to customers, increasing the severity of the risk.

Compromised data can scuttle years of research

Multiple impacts to technology and life sciences companies

Ransomware attacks can result in significant losses for technology and life sciences companies:

- Encrypted systems can immediately cut off valuable workflow of research and development, production and sales.
- Compromised data can scuttle years of research and impact a business's economic viability.
- The potential theft of intellectual property and its subsequent extortion can cost even more than an exorbitant ransom.
- Both industries are highly regulated and a data breach may also result in fines.
- A successful ransomware attack on one technology company that provides software and hardware can quickly spread to thousands of businesses through compromised credentials. That vulnerability can result in potentially thousands of lawsuits and brand damage.

(Return to Table of Contents)

Ransomware vulnerabilities and remote workers.

In its "2021 Threat Predictions Report," McAfee, the global computer security software company, predicts that ransomware attackers will increasingly target remote workers to compromise their employers.[7]

Ransomware attackers have both evolved and multiplied, with RaaS letting any novice attacker bring the full force of ransomware against any susceptible company. When the COVID-19 pandemic hit, tech companies were among the first to move their employees to a remote work situation. That meant that the number of connected devices outside of the workplace increased, which expanded the number of vulnerable endpoints available to launch a ransomware attack.

Relying on a digitally connected remote workforce makes technology companies easier targets

While many technology and life sciences companies are making moves to bring employees back to offices, these industries are still heavily geared to employing remote workers. Relying on a digitally connected remote workforce makes technology companies easier targets for ransomware. If employees are not using company-issued computers, they may not be configured as securely as a company computer, and also may be exposed to malicious websites that may otherwise have been blocked by the company's firewall. When those devices are used for business and personal use, it makes it easier for cybercriminals to infiltrate a company network. For instance, if an employee is using their personal laptop at home for work and opens a personal email that contains ransomware, the gateway is also opened to the corporate network.

Home systems like routers, home computers and smart-home devices may not be up to date and are more vulnerable to compromise. In addition, home networks and endpoint security are not as advanced as corporate IT security systems.

Another vulnerability associated with a remote workforce is the lack of governance. Personally owned computers may not be monitored for suspicious activity. In addition, as more remote employees become isolated from day-to-day corporate administration, they may also become less guarded, paying less attention to warnings and training. With more people working remotely and working irregular hours, it becomes difficult for corporate security teams to identify unusual or suspicious activity.

Employing preventive measures that don't adapt to a remote work situation can make IT companies and electronics manufacturers more vulnerable to ransomware.[8] Remediation costs can add to the financial burden, along with costs to meet daunting state and federal regulatory requirements in the wake of a breach.

(Return to Table of Contents)

How to protect your technology company from ransomware.

There are a number of steps a company should take to defend against a cyberattack, such as ransomware. These important measures are among the first things you should enact:

Step 1 – prepare

- Maintain an inventory of all hardware devices and software applications.
- Keep applications and operating systems up to date.
- Ensure all devices are properly configured and security features are enabled.
- Apply the Principle of Least Privilege to all systems and services so that users only have the access they need to perform their jobs.
- Implement a program to validate security of third-party/supply chain/service providers
- Maintain inventory of all third parties, suppliers and service providers.
- Review your services agreements and understand all terms and conditions.

Effective ransomware protection is multidimensional

Step 2 – prevent

- Ensure antivirus software, spam filters and firewalls are installed and regularly updated.
- Implement an intrusion-detection system to alert you to potential malicious activity prior to ransomware deployment.
- Implement multifactor authentication (MFA).
- Generate, retain and protect logs from network devices and local hosts to support triage and remediation in the event of a ransomware attack.
- Implement a robust security awareness training program, including phishing:
  - Train all employees on how to identify and report suspected phishing emails.
  - Perform phishing simulations to gauge employee awareness and provide training for "clickers."
- Enforce a strong password policy.
- Implement a robust secure Systems Development Life Cycle (SDLC) program:
  - Follow secure coding practices – such as the Open Web Application Security Project® (OWASP) framework.
  - Manage access to source code.
  - Ensure integrity of source code throughout the life cycle.
  - Scan code for vulnerabilities prior to production.

Step 3 – mitigate

- Conduct regular vulnerability scans to find vulnerabilities; patch them ASAP!
- Create, maintain and exercise a cyber incident response plan that includes the following response and alert procedures for a ransomware incident (adapted from CISA MS-ISAC Ransomware Guide):
  - Report the incident.
  - Determine which systems were impacted and immediately isolate them.
  - Triage impacted systems for restoration and recovery.
  - Preserve evidence.
  - Eradicate the malware.
  - Restore systems.
  - Build on lessons learned.

Step 4 – restore

- Maintain current, protected backups of your critical data and IT infrastructure so that you can quickly restore operations.
  - Regularly back up your data and IT infrastructure.
  - Encrypt backups.
  - Keep at least one copy "offline," i.e., not accessible from your network.
  - Regularly test the integrity of your backups and effectiveness of your restoration process.

(Return to Table of Contents)

Smart ways to gain an extra layer of ransomware protection.

If you want to greatly reduce your business's risk associated with ransomware, consider the benefits that come with endpoint detection and response (EDR) systems and MFA.

Passwords and antivirus software alone are no longer enough to protect against malware that can result in ransomware. Adding additional layers of defense, such as EDR and MFA, can play a key role in stopping or slowing ransomware attacks.

More and more tech companies have ransomware safeguards

What you need to know about EDR

Antivirus software is a help in protecting your systems. But if antivirus is your only defense, you should give serious consideration to upgrading to an EDR solution. This type of integrated solution provides more robust capabilities than traditional antivirus in protecting against attacks by monitoring for abnormal behavior on each system rather than simply searching for known malware.

What you need to know about MFA

MFA requires that a user authorized to access your system use more than one method to validate their identity. For example, to log in, in addition to a user ID and password, they must also provide a PIN, a fingerprint or a one-time password provided by text, or an application, such as Google Authenticator. This safety protocol can help prevent malware and ransomware from spreading from one computer to an entire network.

MFA is important but the options for how to implement it can vary from one environment to the next. Travelers CyberRisk policyholders can access a one-hour consultation with a Symantec™ Cyber Security Coach who can provide much-needed expertise and help pave the way for a smooth MFA implementation, and a stronger cybersecurity program.

(Return to Table of Contents)

Why technology companies should have cyber insurance.

Technology companies might face greater exposure from cyberattacks, including ransomware attacks, because of the potential added impact to customers who rely on their services.

This is why technology companies and organizations need to be prepared with an effective cybersecurity program to manage cyber risks that includes cyber insurance.

What would a ransomware attack do to your company?

What coverages should technology companies look for in cyber insurance? In addition to the cost of a ransom demand, it should cover the many types of expenses that can result from a cyberattack.

Those include:

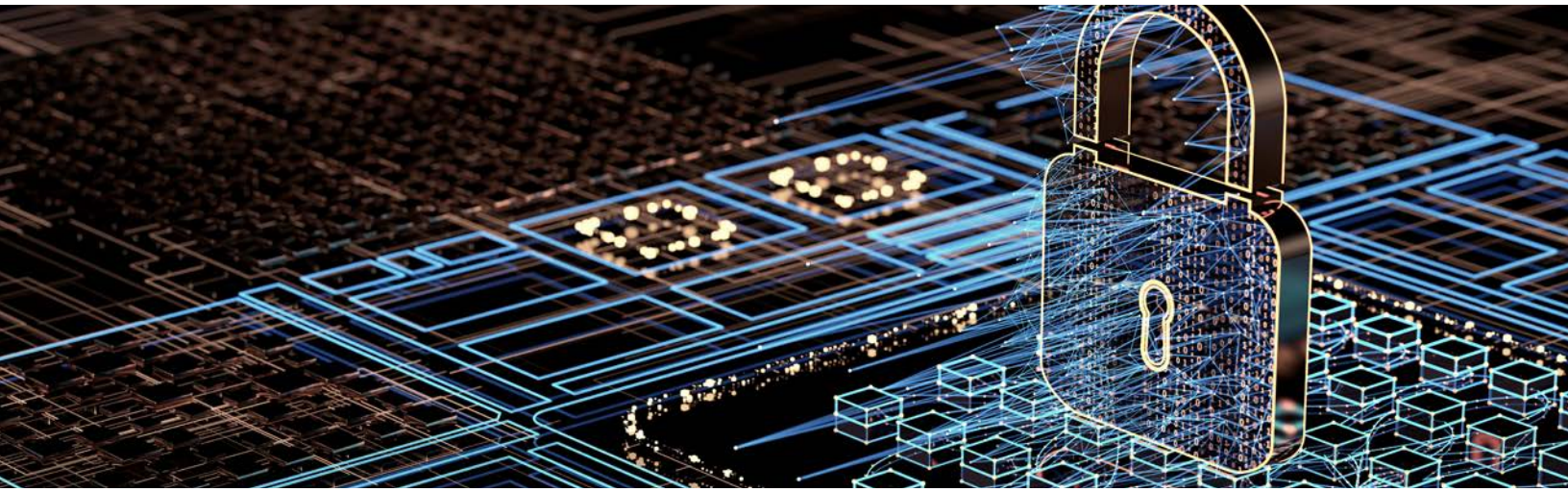
- Data restoration.
- Lost income.
- Forensic investigations and remediation.
- Legal costs for privacy counsel to coordinate the response to a cyberattack.
- Regulatory defense expenses and fines.
- Public relations services.
- Costs to improve a computer system after a security breach, when improvements are recommended to eliminate vulnerabilities that could lead to further breaches.

If you are a global technology company, make sure you are aware of any regional restrictions to coverage.

Cyber coverages are an important complement to Technology Errors & Omissions (E&O) that all technology companies should also have.

Look for a provider who has a track record for fast response, knowledgeable and professional claims management, and specific experience in the types of losses that can leave tech companies most vulnerable.

(Return to Table of Contents)



What cyber insurance typically does not cover.

Cyber insurance is not a panacea for ransomware and is not intended to replace an upfront investment in security controls. Cyber insurance typically does not cover:

- Potential future lost profits.
- Loss of value due to theft of intellectual property.
- Property damage.
- Cost to restore computer systems and networks to a higher level of functionality.

Every organization's cyber risk is different

Travelers CyberRisk Tech Coverage for technology companies is a powerful modular approach to writing coverage that is broad enough – and flexible enough – to meet the complex needs of today's state-of-the-art technology companies.

CyberRisk Tech Coverage offers the following insuring agreements:

Liability Coverages, including:
Technology Errors & Omissions
Privacy and Security
Regulatory Proceedings

Breach Response Coverages, including:
Privacy Breach Notification
Cyber Extortion
Data Restoration

Cyber Crime Coverages, including:
Computer Fraud
Funds Transfer Fraud
Social Engineering Fraud

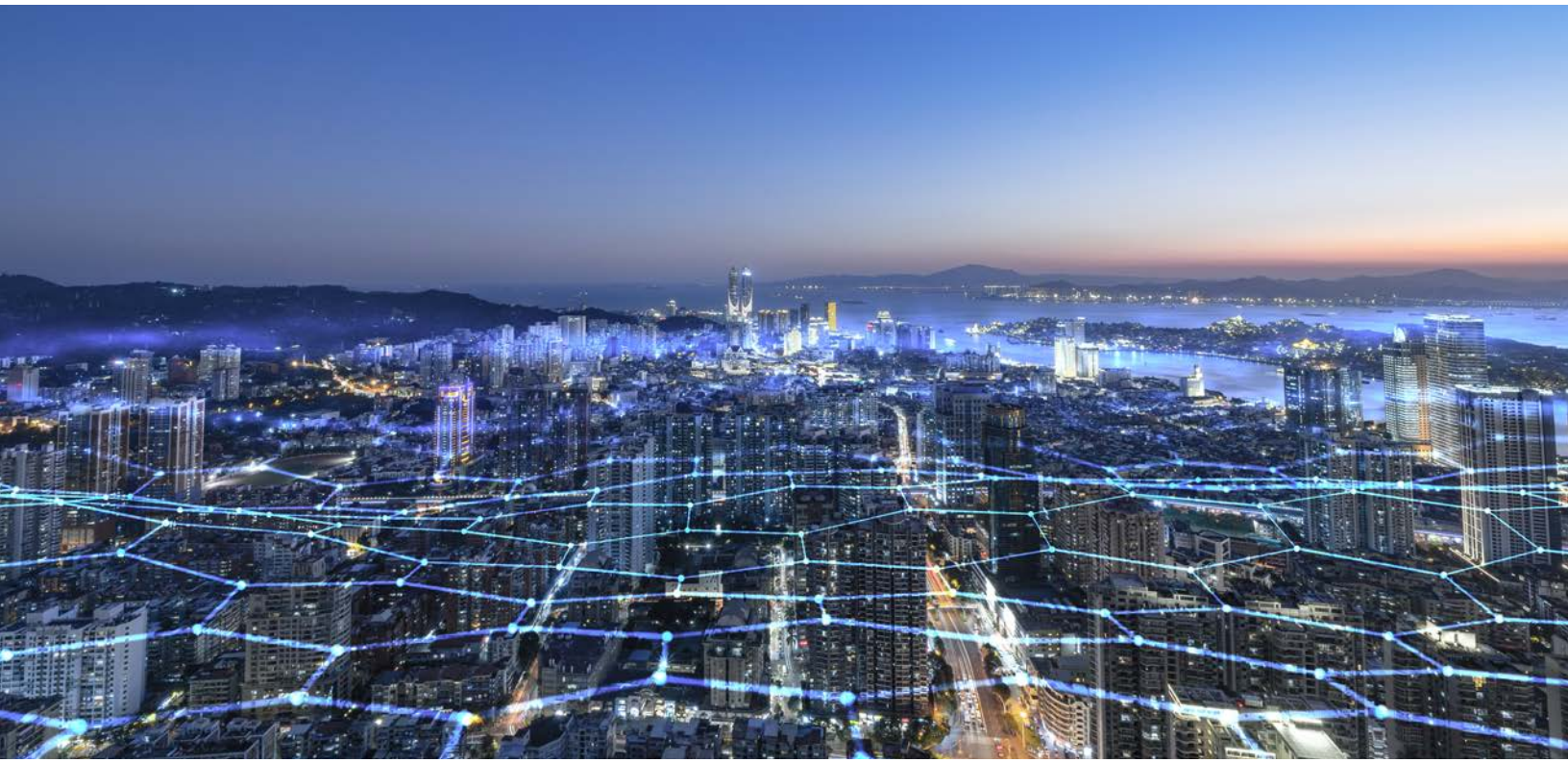
Business Loss Coverages, including:
Business Interruption
System Failure

Every organization's cyber risk is different. It's important to understand what your risks are as well as the options available that can protect your data and your organization from ransomware.

Actions to take:

- Learn how to do a cyber risk pressure test.[9]
- Gain insight into the current ransomware landscape.[10]
- Understand the benefits of cyber insurance.[11]

(Return to Table of Contents)



Sources:

[1] "Kaseya, the tech firm hit by ransomware, gets the key to unlock its customers' data." – New York Times

[2] "sDoppelPaymer Ransomware Attack Disrupts Foxconn's Operations in the Americas, Hackers Delete Terabytes of Data, Demand $34 Million" – CPO Magazine

[3] "Acer reportedly hit with $50 million ransomware demand" – The Verge

[4] "Technology giant Olympus hit by BlackMatter ransomware"– TechCrunch

[5] "AI Wrote Better Phishing Emails Than Humans in a Recent Test" – Wired Magazine

[6] "Ransomware can cost firms over $700,000; cloud computing may provide the protection they need" – CNBC

[7] "2021 Threat Predictions Report" – McAfee

[8] "5 Cyber Risks for Technology Companies" – Travelers.com

[9] "The Cyber Risk Pressure Test" – Travelers.com

[10] "What Is the Current Ransomware Landscape?" [Video & Infographic] – Travelers.com

[11] "Travelers Cyber Insurance Solutions" – Travelers.com

TRAVELERS

travelers.com