PERSPECTIVES

RANSOM! THE UNFORTUNATE NEW NORMAL:
CYBERSECURITY CONSIDERATIONS FOR FIDUCIARIES

SECOND EDITION

JS|HELD

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

thebrief™ | JS|HELD

Court-appointed receivers, chief restructuring officers, distressed asset investors, and lenders should read this article to:

- Realize that cybersecurity is now a fiduciary duty and should be incorporated into every engagement alongside protection of cash, collateral, and physical assets.
- Understand that immediate onboarding assessments should include digital infrastructure, privileged access controls, remote connections, backups, email security, and cyber insurance reviews.
- Recognize that proactive IT lockdowns and access management can significantly reduce ransomware exposure and safeguard enterprise value.
- Acknowledge that business interruption consequences often create larger losses than the ransom itself and can derail a restructuring or sale process.
- Know that effective contingency planning improves resilience, reduces downtime, and enhances the likelihood of successful engagement outcomes.

Insurance carriers and cyber claims professionals should read this article to:

- Understand that cyber business interruption is frequently one of the largest components of cyber-related financial losses and insurance claims.
- Understand that organizations should evaluate insurance adequacy before an event occurs, as many businesses remain materially underinsured for cyber incidents.
- Learn that financial damages can include restoration costs, income loss, regulatory investigations, litigation exposure, forensic expenses, incremental expenses, and reputational harm.
- Know that forensic accounting expertise is essential in quantifying business interruption during a cyber ransomware incident.
- Understand that risk assessments should address both direct cyber threats and third-party operational dependencies that can trigger significant business interruption losses.

EXPERT VOICES

Jake Dilorio, CTP

Jake explains why ransomware has become a fiduciary risk management issue, drawing on his restructuring and receivership experience to outline how fiduciaries can secure digital assets, control cyber exposures, and protect enterprise value during distressed engagements.

Jessica Eldridge

Jessica examines the often-overlooked financial consequences of ransomware, applying her forensic accounting and cyber business interruption expertise, and shows how operational disruptions, recovery costs, and insurance gaps can significantly increase losses after an attack.

Executive Summary

Ransomware has become a persistent business risk that fiduciaries, receivers, and restructuring professionals must address in every engagement. Several high-profile incidents affecting organizations across healthcare, manufacturing, food production, and critical infrastructure illustrate the rapid growth of ransomware and its serious financial impact. Smaller and financially distressed companies are especially vulnerable because they often lack the resources to maintain robust cybersecurity defenses and comprehensive cyber insurance coverage.

This article explains that effective risk management begins with assessing digital infrastructure, remote access systems, email security, and business interruption exposures before an attack occurs. Through examples and practical guidance, it demonstrates how proactive planning, contingency strategies, IT lockdown procedures, data backups, monitoring tools, and insurance reviews can significantly reduce operational and financial losses. Cybersecurity that recognizes the risk of ransomware has become a core fiduciary responsibility, and organizations that prioritize prevention, resilience, and continuous monitoring are better positioned to survive such cyber extortion events and protect stakeholder value.

Introduction

The order was signed a week ago. When your team arrived on-site and turned on the controller's computer, they were greeted with a skull-and-crossbones-themed message:

"Your files have been encrypted. You must pay a $10 million ransom within 48 hours to regain access to your files. To restore your system, email I-own-you@aol.com and include your new Account ID Aug2027_246 in the subject line. Payment instructions will be provided."

Ransomware threats have become commonplace. Management and executive leadership should be aware of the emerging best practices to protect their companies from falling victim to the latest ransomware attacks.

Cyber Risk & Ransomware Equal Enterprise Risk

Cybercrime continues to rise at an alarming pace. According to Statista, global losses from all forms of cybercrime reached approximately USD 10.29 trillion in 2025 and are projected to exceed USD 16 trillion by 2029.

Among the many types of cybercrime, ransomware remains one of the most pervasive threats. Verizon's *2025 Data Breach Investigations* Report found that ransomware was involved in 44% of all data breaches. At the same time, organizations are becoming more resistant to extortion demands.

Despite this growing reluctance to pay, the financial impact of ransomware continues to escalate. According to Cybersecurity Ventures, ransomware damages are expected to reach USD 74 billion in 2026 and surpass USD 275 billion globally by 2031. The report also noted that 69% of victims now refuse to pay ransoms, and the median payment has fallen to USD 139,875, down from USD 150,000.

The effects are also being felt in the United States. In 2025, the FBI's Internet Crime Complaint Center received more than 3,600 ransomware-related complaints, with reported losses exceeding USD 32 million. Together, these figures highlight both the growing scale of the ransomware threat and the increasing determination of organizations to resist paying cybercriminals.

At the same time, this shows that ransomware attacks are ***not*** slowing down. Some of the most serious and recent ransomware attacks include:

- **July 16, 2026:** fairlife LLC, a Chicago-based dairy company owned by Coca-Cola, was hit with a ransomware attack, according to a regulatory filing with the US Securities and Exchange Commission. The amount requested for the ransom was unspecified in the filing. However, Coca-Cola stated that it "identified unauthorized access by a third party to a portion of its systems, including its production-related systems, in connection with a ransomware event. After detecting the issue, [Coca-Cola] promptly activated its incident response and business continuity protocols." The food and beverage giant said it has notified law enforcement and that its

dairy unit's "product quality and safety have not been impacted." However, following the incident, fairlife's US production operations were temporarily suspended. Coca-Cola further stated that it "has not yet determined whether the incident is reasonably likely to materially affect the Company."

- **January 27, 2025 to February 6, 2025:** Episource, a medical coding vendor and subsidiary of UnitedHealth Group's Optum division, suffered a suspected ransomware attack that led to a data breach exposing the personal information of 5.4 million people. The ransom amount was unspecified.
- **February 21, 2024:** The UnitedHealth Group's Change Healthcare was attacked by a ransomware group known as ALPHV BlackCat. This became known as one of the largest cyberattacks on the US healthcare industry. The company reportedly paid a USD 22 million ransom. The attackers took the money but never delivered the information. UnitedHealth estimated that costs from the attack could exceed USD 1 billion.

While high-profile cybersecurity attacks like these make the headlines, most attacks hit small, private companies. Small and medium-sized businesses are disproportionally affected by ransomware attacks, the Verizon report noted. In the United Kingdom, more than 50% of the 323 organizations that reported a ransomware attack between April 2025 and March 2026 were small or medium-sized businesses.

Most are privately held companies like those we represent as receivers and restructuring professionals. After all, investing in state-of-the-art IT security is unlikely when a business is in financial distress. Hence, it is imperative for fiduciaries to understand the leading indicators of cybersecurity threats and how to respond.

Cryptocurrency: The Fuel Behind Ransomware Attacks

Cybercriminals have been hacking into computers for decades, but the rise of cryptocurrency has significantly increased the access, frequency, and economic incentives behind ransomware attacks. Cryptocurrency enables bad actors to demand and receive ransom payments across borders with relative anonymity, reducing the likelihood of recovery or prosecution. While fiduciaries cannot control the existence of cryptocurrency or the evolving threat landscape, they can identify and secure the pathways that cybercriminals commonly exploit.

For court-appointed fiduciaries, receivers, trustees, chief restructuring officers, and other interim executives, as with all companies, cybersecurity should be treated with the same urgency as securing cash, collateral, and physical assets. The onboarding processes for new engagements should include assessments of:

- **Digital Infrastructure and Critical Systems:** Cloud-based software, data repositories, Microsoft 365 and Google Workspace environments, ERP systems, accounting platforms, websites, domain registrations, inventory systems, customer databases, and any other critical applications of the business requiring a login name and password.
- **Administrative Access and Identity Controls:** Identification and control of all privileged accounts, including domain administrators, global administrators, cloud administrators, and third-party IT providers. Multi-factor authentication (MFA) should be implemented wherever possible; access for former employees and owners should be reviewed and removed, and administrative credentials should be secured immediately.

- **Remote Desktops, VPNs, and Third-Party Connections:** Remote desktops and virtual private networks (VPNs) continue to be commonplace in today's workplace and are one of the most common attack vectors. Some are poorly installed, providing an easy point of entry for hackers. This review should include an inventory and assessment of remote monitoring tools, vendor access, and other external connections.
- **Email Security and User Access:** Email systems remain a primary vehicle for phishing, credential theft, and other threats. Fiduciaries should evaluate email security controls, identify suspicious forwarding rules, confirm account ownership, and assess tools designed to detect phishing attempts, spoofed addresses, and malicious attachments.
- **Data Preservation and Backup Integrity:** Before significant system changes are made, fiduciaries should inventory critical data and verify that recoverable backups exist. Equally important is confirming that backups can actually be restored if needed. Consideration should also be given to data preservation requirements, litigation holds, and the maintenance of records that may become relevant in future disputes or investigations.
- **Cyber Insurance and Incident Preparedness:** Fiduciaries should review cyber insurance coverage, ransomware coverage, incident response resources, and business interruption protections early in the engagement. Some distressed companies may maintain only minimal cyber coverage, which may be inadequate to address a significant breach or ransomware event.

Cyber risks continue to evolve, but the basic underlying protocols shall not waiver: fiduciaries must quickly establish control over both physical and digital assets. In today's environment, securing administrative access, validating backups, monitoring remote connections, and protecting sensitive data are as critical to preserving enterprise value as safeguarding cash and inventory. A successful engagement now requires not only operational and financial stabilization but also deliberate protection of the organization's digital infrastructure and information assets.

Top Industry Targets for Ransomware

- Professional services (small to medium size)
- Healthcare/medical
  - Data
- Education organizations
  - Intellectual Property from campus research
- Personal information/data
  - Energy/utilities
- Banking/financial services

Cryptocurrency: The Fuel Behind Ransomware Attacks

Nefarious people worldwide have been hacking into computers for decades. The advent of cryptocurrency elevated hacking to a whole new level. This difficult-to-trace currency enables thieves to receive ransom without payment tracking and—more importantly—prosecution for their criminal acts. You can't control the existence of cryptocurrency, but you can assess the doorways thieves are using to gain access to systems.

Your onboarding processes for new engagements should include assessments of:

- **Digital Infrastructures:** Cloud-based software and storage, websites, inventory systems, and any other business methods requiring a login name and password.

- **Remote Desktops and VPNs:** Thanks to the global pandemic, remote desktops and VPNs are ubiquitous. Some are poorly installed, providing an easy point of entry for hackers.
- **Email:** Protocols and software tools to identify phishing and other questionable inbound emails and spoofed email addresses.

Planning Before Disruption Occurs

Organizations should plan for business interruption before an incident occurs. While no company can prevent every disruption, effective planning can reduce costs, shorten downtime, and, in some cases, determine whether the business survives a crisis.

- For example, consider a small manufacturer that depends on third-party software and equipment to track lot numbers and stamp finished products with required traceability information. If that supplier suffers a ransomware event, the manufacturer may be unable to ship the products. If it supplies a major original equipment maker, the resulting penalties and delays could threaten its survival within days unless effective contingency plans are already in place.

With advance planning, the manufacturer likely would have identified lot traceability as a critical production requirement. It could then have secured a backup supplier or developed a manual process to keep production moving while an alternative solution was implemented.

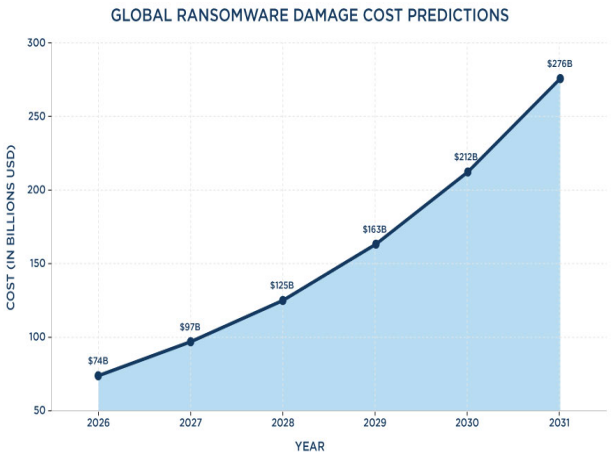
- In another example, a large pharmaceutical company suffers a ransomware attack that encrypts multiple servers, including its backups. It must divert lab services to other facilities while critical devices are unavailable. Sensitive patient information is also compromised and exfiltrated. Even after paying a ransom, the company takes more than a month to become fully operational again. The resulting restoration costs, income loss, and additional expenses can exceed millions of dollars, not including the multi-million-dollar ransom payment or the costs of breach counsel, forensic investigations, patient notifications, regulatory investigations, and third-party class-action defense and settlement.

These costs accumulate quickly, making it critical for businesses to conduct due diligence before an event to confirm they have adequate insurance coverage and an incident response plan in place.

The True Cost of an Attack

In many cases, the largest losses are driven by operational disruption rather than the ransom itself. Cyberattacks can halt production, disrupt supply chains, disable critical systems, and cause substantial business interruption and additional expense losses.

In addition to the ransom, the costs of a cybersecurity attack include lost revenue from customers and new leads, as well as from being offline. The company may face extraordinary costs by hiring expert IT consultants to assess the damage and remedy the IT infrastructure.



Source: Cybersecurityventures.com

Even a modest, 10-employee business could experience a six-figure ransom demand. A USD 100,000 ransom payment or USD 50,000 in lost business could be the difference between making payroll to carry the company through a going-concern sale process and ceasing operations due to a lack of cash flow.

Action Plan

Your first step must be to assess your company's risk of a cyberattack. Reassess your IT protocols to protect your business. A cybersecurity threat can directly impact the outcomes of your engagements and could bring them to an abrupt halt, damaging your wallet and your reputation. Also, make sure you have adequate cyber insurance.

When it comes to the organizations you oversee, each must be secure enough to deter hackers. Develop relationships with IT consultants with cybersecurity expertise. Get a roadmap from them for your new-engagement onboarding assessment and bring them in when you identify potential risks.

What are your immediate priorities?

1. Identify and secure all cash and limit banking access to key people.

2. Identify and secure all assets/collateral of the receivership estate.

3. Lock down the IT environment and stress-test the system using a qualified IT professional to identify any weaknesses in the firewalls, etc.

4. Identify insurance coverages and assess adequacy of coverage.

The first two action items are second nature for most of us, but the third and fourth are a bit murkier and may require a comprehensive understanding of the business and its customers, as well as employee/customer/vendor access to its VPN and more.

Example: Consider a receivership matter in which the business was assessed for vulnerability to ransomware attacks. Under such an analysis, there may be a complete IT lockdown after securing all access points to the IT infrastructure, including blocking access by former employees and third parties. What follows are three critical IT tasks:

1. Obtaining "3-2-1" backups of all data (3 backups, 2 different devices, 1 being offsite).

2. Establishing a firewall with monitoring of all traffic.

3. Reviewing the need for monitoring of all computers and servers with Advanced Antivirus (AV) and Remote Monitoring & Management (RMM) tools.

The business's insurance coverages may also need to be reviewed, especially its cyber insurance coverage, to see whether a rider limits coverage to its general liability policy. If such a rider had existed when the company was hacked, insurance coverage would have been inconsequential. A ransomware or cyber incident would have frozen operations.

However, implementing the three tasks above may substantially reduce the risk of a ransomware attack or other cybersecurity breach. The risk of a costly business interruption event would be substantially reduced, enabling the successful completion of an engagement.

Why Cyber Business Interruption Matters

Cyber business interruption includes lost business income and increased operating expenses caused by a cyber event that disrupts operations. It is often one of the largest components of a cyber insurance claim because

organizations increasingly rely on technology, connected systems, and third-party service providers to operate.

Conclusion: Your New Normal

In today's threat environment, proactive cybersecurity is essential. Organizations that emphasize prevention, early detection, and continuous monitoring are better positioned to withstand cyber incidents and recover quickly. The key considerations for protecting against ransomware attacks and their financial impact in the receivership environment are:

1. Careful configuration of remote working arrangements. According to securitymagazine.com, hackers prey on remote work environments and human error to steal corporate data.

2. Assess cyber insurance coverage. Some businesses may believe they are covered, but they simply have a USD 5,000 or USD 10,000 rider to their general liability policy.

3. Assess the IT infrastructure, including personnel training, software, and hardware. Is it sufficiently robust for the business?

The new normal is here, but questions remain about how it will evolve: whether fiduciaries will need cybersecurity experts on staff, whether government intervention will increase, and whether cryptocurrency will continue to create conditions that make ransomware easier to exploit. At the same time, AI is making ransomware faster and more dangerous by helping attackers break into systems, launch attacks quickly, evade detection, create convincing phishing messages, clone executive voices, and identify valuable data to steal or leak.

Acknowledgements

We would like to thank our colleagues, Jake Dilorio and Jessica Eldridge, for providing insight and expertise that greatly assisted this research.

Jake Dilorio is a Senior Managing Director in J.S. Held's Strategic Advisory practice, having joined J.S. Held's Strategic Advisory Group in October of 2024 as part of J.S. Held's acquisition of Stapleton Group. Jake is a certified treasury professional (CTP) and a seasoned restructuring expert and court-appointed fiduciary, instrumental in resolving complex turnarounds, receiverships, and loan workouts for operating businesses and real estate entities. He designs and implements strategies to repair fractured relationships among debtors, creditors, and other stakeholders, achieving the best outcomes for all parties. Jake applies his extensive experience as a fiduciary managing projects ranging from solvency analyses to comprehensive receiverships and Chapter 11 restructurings. He works closely with management to assess financial and operational viability and design the optimal path to recovery, which may include recapitalizations, going-concern sales, asset dispositions, and liquidations. He provides clients with key reports throughout the process to facilitate informed decisions.

Jake can be reached at
jake.diiorio@jsheld.com or
+1 213 235 0609.

Jessica Eldridge is a Senior Vice President in J.S. Held's Forensic Accounting - Insurance Services practice. Jessica has over 20 years of investigative and forensic accounting experience in measuring financial damages involving business interruption, cyber, extra expense, stock, builder's risk, employee dishonesty/fidelity, personal injury, subrogation, and litigation support services. Jessica also has extensive experience with the administration of common fee funds and the oversight of property damage claims for large construction

projects. Her industry experience includes, but is not limited to, automotive, life sciences, hospitality, manufacturing, retail, medical services, hospitals, college & universities, casinos, state and local municipalities, specialty human services, recycling plants, real estate, and construction projects.

Jessica can be reached at
jeldridge@jsheld.com or
+1 857 219 5720.