VISUAL EDGE IT™
SECURE TECHNOLOGY SOLUTIONS

LEADERSHIP SERIES

CYBER INSURANCE, RISK MANAGEMENT, AND REGULATORY COMPLIANCE

Aligning Coverage for a Stronger Security Posture

JUNE 2025

www.VisualEdgeIT.com

Contents

Visual Edge IT | 3874 Highland Park NW | North Canton, OH 44720
(800) 828.4801 | www.visualedgeit.com

Introduction

In its October 2024 *Report on the Cyber Insurance Market*, the National Association of Insurance Commissioners (NAIC) cited data showing a 20% increase in the number of cybercrime claims among U.S. businesses from mid-year 2022 to mid-year 2023. Of those claims, 72% showed an increase in severity, indicating that cyber threats and attacks had become more frequent, volatile, and complex. Especially with technologies like AI and Ransomware as a Service (RaaS) emerging as intelligent new tools for online criminals, the upsurge in incidents and their severity was a notable alarm.

A stronger security posture via risk management

As a countermeasure, many cyber insurers began to focus more intently on the risk management practices of the organizations they insured. Today, this approach continues to help businesses of all kinds 1) ease the severity of claims they make for cyber incidents, and 2) reduce the losses from a breach or attack and any resulting operational disruptions. (This formula also benefits the insurer when payouts for claims are less.)

Rather than viewing cyber insurance as a post-incident security blanket, then, businesses should now see coverage as being central to a more vigorous cybersecurity and risk management strategy. By compelling businesses themselves to amplify their risk management practices, cyber insurance more directly augments measures such as risk assessments, advanced security technologies, regulatory compliance, and employee training to form a stronger wall of protection against modern cyber threats.

Reasons Organizations Obtain Cyber Insurance

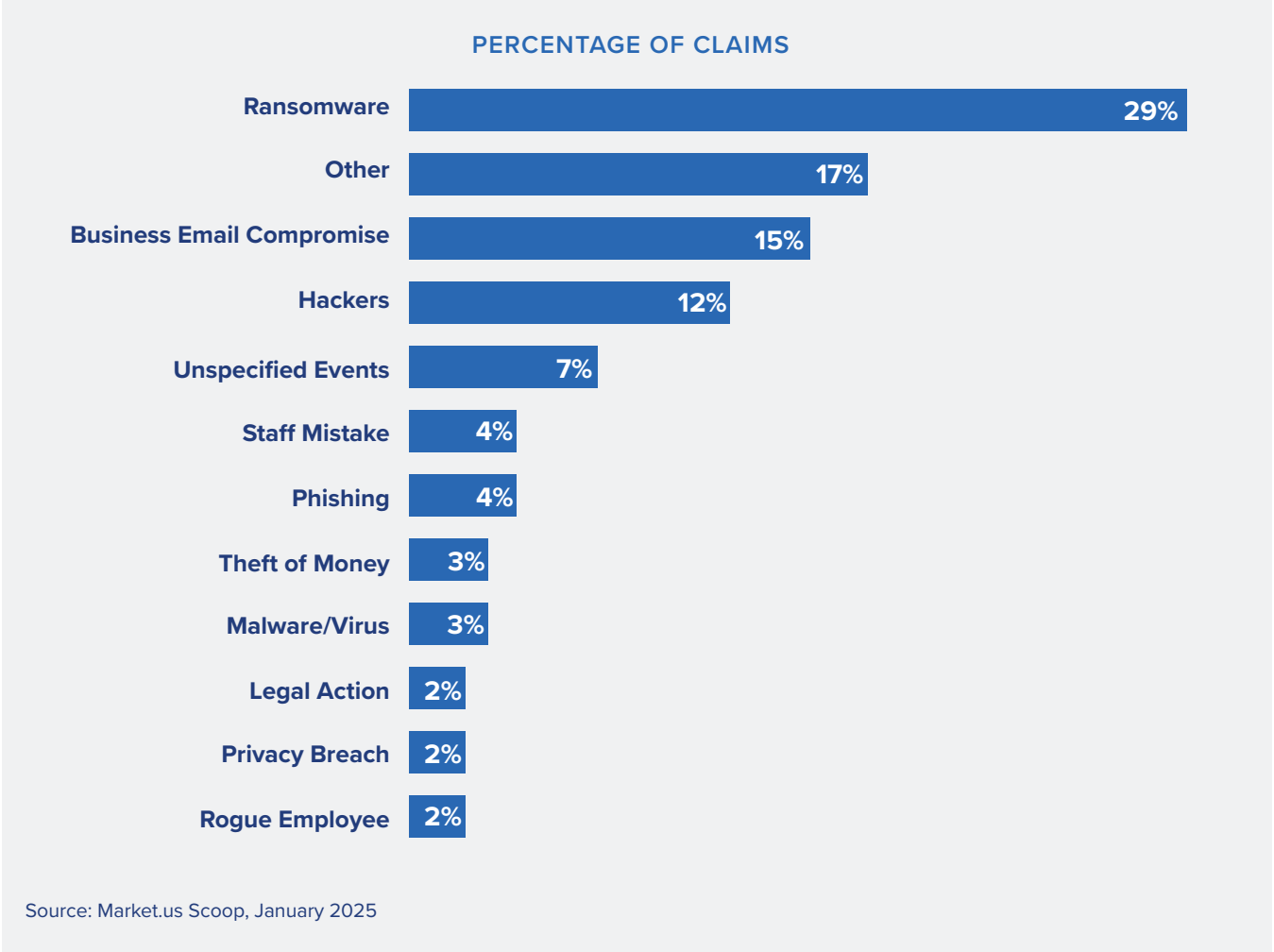
While organizations have various needs for cyber insurance (also often referred to as cybersecurity insurance, cyber liability insurance, or data breach insurance), the following objectives are common drivers to obtain coverage for cyber threats and potential attacks:

- **Financial protection and recovery.** Cyber insurance covers costs for incident response, system and data recovery, legal fees, and so on. Cyber policies also commonly cover any losses incurred from a ransomware attack.
- **Increasing cyber-attack frequency, sophistication, and severity.** AI and other advanced technologies continue to make cybercrime more dynamic, and virtually any business is a constant target.
- **Regulatory compliance.** Cyber insurance is required to meet compliance guidelines for regulations such as the Health Insurance Portability and Accountability Act (HIPAA). In instances of non-compliance, a cyber policy typically covers the costs of regulatory investigations and penalties.
- **Mandates from leadership.** Business leaders make cyber insurance a directive largely for risk management, prevention, and recovery strategies to protect their company and customers.

- **Safeguarding reputation and customer trust.** In the event of a breach, insurance helps cover costs for PR, customer notifications, credit monitoring, and other efforts to reinforce trust.
- **Third-party contract requirements.** Partners and suppliers frequently require a business to maintain cyber insurance as a condition for collaboration, particularly when large volumes of customer data are involved.

Leading Causes of Cyber Insurance Claims

Trends in the types of cyber-attacks and correlating volume of claims continue to shape the cyber insurance market. The threats listed here underscore the need for adaptive cyber insurance solutions.



Source: Market.us Scoop, January 2025

Cyber Insurance Basics

Commonly Covered Cyber Risks

Cyber insurance typically includes first-party coverage of losses incurred through data destruction, hacking, data extortion, and data theft. Although cyber policies vary by provider and plan, they customarily cover the following aspects of security and recovery:

- **Incident response.** Covers the cost of incident response teams to conduct post-attack forensic investigation and recovery efforts. Most insurers facilitate these activities directly to help maintain business continuity and expedite recovery.
- **Customer notifications, reputational protection.** Especially when a breach involves the loss or theft of customers' personally identifiable information (PII). Most policies cover PR and external communications efforts, plus alerts, fraud protection and credit monitoring services for affected customers.
- **System damage repair.** Including networks, servers, computer systems, and other parts of an IT infrastructure damaged by a cyber-attack.
- **Third-party risk.** Recovers costs and revenue losses incurred from attacks on third-party vendors (partners and suppliers) that have access to business data.
- **Regulatory fines.** Ensures the payment of fines when a business is non-compliant with applicable industry regulations.
- **Legal fees and court costs.** Pays attorney and court fees associated with legal proceedings, as well as settlements and court judgments.
- **Ransom demands.** Covers the costs of meeting extortion demands, although most cybersecurity experts advise against paying ransoms.

Risks Often Excluded from Coverage

Even as insurers increasingly focus on the risk management practices of the businesses they insure, a cyber insurance policy will sometimes exclude issues considered to be preventable or caused by human error or negligence, such as:

- **Poor security processes.** When an attack occurred due to poor configuration management or having ineffective security processes in place.
- **Preexisting vulnerabilities.** When an organization suffers a data breach as the result of failing to address or correct previously known vulnerabilities.
- **Human error, ineffective employee training**. When a cyber-attack is traced to human error, often the result of insufficient employee training for cybersecurity.
- **Insider attacks.** When the loss or theft of data results from an insider attack, either executed or coordinated by an employee.

Exclusionary Language

In line with risks excluded from cyber insurance coverage, many cyber policies contain exclusionary language to limit the insurer's liability for certain types of risks. For instance, some carriers include an exclusion referred to as the "failure to maintain security" or "failure to follow adequate security standards." (We listed this as poor security processes in the previous section.) Other cyber policies issued in the U.S. even include "war and hostile act" exclusions, which stipulate that an insurer will not cover losses resulting from acts of war, terrorism, or other hostile actions outside the realm of a cyber-attack.

Where General Liability Policies Fall Short

As somewhat of a stopgap for cyber insurance, some businesses simply attach a rider for cybersecurity to the general liability policy they maintain for normal operations. This type of rider for security typically ranges from $150,000 to $200,000. However, while such riders pay for issues like recovering a backup system after a data breach, they do not cover the cost of services like forensic investigations. The expense of determining the source of an attack or even paying legal fees in a related lawsuit is why a business should carry a sufficient amount of cyber insurance separately.

Applying for Cyber Coverage: Responsibilities for Businesses

Because the guidelines for obtaining coverage constantly change — and given the increased emphasis on a business's risk management practices — applying for cyber insurance itself is complex. To complete the application process, most insurers require an organization to implement and verify the following security measures.

- **Endpoint detection and response (EDR)**, implemented on all endpoints.
- **Multi-factor authentication (MFA)**, implemented for critical systems and users.
- **Backup procedures**, whether offline or using alternative solutions such as the cloud.
- **Identity and access management (IAM)** for ad-hoc privileges and restricted network access.
- **Privileged access management (PAM)** to monitor accounts with privileged access.

Good examples for system and user verifications are EDR and MFA. For EDR, organizations must make sure the product they use meets the insurer's EDR requirement and is installed on all endpoints. (Don't assume EDR is implemented on every endpoint.) Similarly for MFA, in addition to software accounts like Office 365 that inherently require MFA for each user, insurers require an organization to verify that office equipment such as multi-function printers and copiers are also MFA-protected.

Application Process Checklist

- ☐ **Assess organizational cyber risks.** Identify critical assets, understand potential vulnerabilities, and assess the impact of potential cyber incidents on your operations.
- ☐ **Implement robust cybersecurity measures.** In addition to EDR, MFA, IAM, PAM, and backup procedures (stated earlier), ensure measures such as regular security audits, employee training, and data encryption to reduce risks.
- ☐ **Gather necessary documentation.** Documentation should demonstrate your organization's cybersecurity posture, including general liability policies, incident response plans, and any records of past security incidents. This information helps insurers assess your risk profile.
- ☐ **Engage with insurance providers.** Consult with insurance providers to understand available cyber insurance products. Or, work with an independent broker who can assist in tailoring policies to your organization's specific needs.
- ☐ **Obtain and compare quotes.** Request quotes from multiple insurers to compare coverage options, premiums, deductibles, and policy limits. Ensure that the policy aligns with your identified risks and budget.
- ☐ **Review and finalize the policy.** Carefully review the terms and conditions of the proposed policy, including coverage limits, exclusions, and the claims process. Once satisfied, finalize the policy and ensure that all stakeholders are informed.

Risk Management

Again, with the increasing frequency and sophistication of cyber-attacks, risk management has become more essential both to a business's cybersecurity strategy and to insurers who provide cyber coverage. Beginning with a security risk assessment, managing risk should be an ongoing process, as well as a continuous priority.

A Comprehensive Risk Assessment

As a top best practice to gauge cybersecurity risk, a comprehensive risk assessment enables a business to:

- Identify potential vulnerabilities and threats to information systems, including networks, cloud-based systems, and mobile devices.
- Evaluate the likelihood and impact of all detected risks, especially for remote and work-at-home employees.
- Develop appropriate mitigation strategies.

As any security professional will verify, simply having security software, firewalls and MFA in place is not a security strategy. Along with a risk assessment, a security strategy should align with a business's objectives to protect critical systems and data, and requires an expert to help contrast such objectives, particularly for cyber insurance needs. Many times, a strategy is built on industry best practices, or on compliance frameworks such as the Cybersecurity Maturity Model Certification (CMMC), the Payment Card Industry Data Security Standard (PCI DSS), or HIPAA.

A Repetitive Process

While the results of a risk assessment help solve gaps in security, the process should be a repetitive one. For instance, an initial assessment might uncover system weak spots vulnerable to malware and ransomware, but not to Denial-of-Device (DoS) attacks or Advanced Persistent Threats (APTs). At this point, in an effort to identify other potential risks, an assessment requires "changing the rules" to make the process harder.

The goal is to disrupt security procedures and business continuity plans as much as possible for all likely risks. By doing so, businesses can determine exactly how they'll overcome any and all challenges that result because of risk.

Risk Assessment Steps

Source: Hyperproof

A Multilayered Approach to Security

Another best practice in risk management is to implement a multilayered approach to security. This involves using a combination of the following controls.

- **Technical controls** include firewalls, antivirus software, and intrusion detection systems.
- **Administrative controls** involve policies, procedures, and training programs to educate employees on cybersecurity best practices and ensure compliance with security protocols. These controls are particularly critical when employees work remotely.
- **Physical controls** include measures such as access controls and video surveillance to protect against physical breaches.

By implementing a multilayered approach such as this, businesses reduce the likelihood and impact of cyber-attacks. They also further ensure the confidentiality, integrity, and availability of critical information assets.

Regulatory Compliance

Compliance and Insurance Frameworks

For cybersecurity compliance, organizations are required to conduct a security risk assessment that adheres to a specific regulatory framework such as HIPAA or the National Institute of Standards and Technology (NIST). An auditor conducting this assessment can either determine that an organization meets all stated framework requirements, or expose gaps and recommend ways to remedy them to meet the specific type of compliance.

Insurers likewise require an organization to adopt a framework for cyber insurance, and typically impose one of two types. The first is a *self-imposed framework* for good security hygiene and business practices that provide basic, well-designed requirements to start. The other is the *NIST Cybersecurity Framework*, or NIST CSF 2.0 (as of February 2024), which requires third-party attestation that an organization meets the updated 2.0 governance requirement for managing and reducing cybersecurity risk.

Essentially, insurance companies want to know if an organization has taken a broad look at cybersecurity, and whether that organization is implementing a sound security posture that aligns with its self-assessment.

Industry-Specific Requirements

Many industries susceptible to cyber-attacks have made cyber insurance a compliance requirement. The healthcare industry, for instance, now requires all providers regulated by HIPAA to carry dedicated cyber coverage. Banks and credit unions (on a state-by-state basis) also must build cyber insurance into their overall coverage as required by the Federal Deposit Insurance Corporation (FDIC). Additionally in critical energy sectors, coverage is mandated by regulations such as NIST, CMMC, and others. Cyber insurance in these cases provides an added wall of financial and compliance protection to safeguard patients and customers as well as organizations.

Non-Compliance Violations

The consequences of non-compliance with cybersecurity regulations can be severe. Businesses found in violation can incur legal and financial penalties from regulatory agencies, as well as reputational damage and a loss of business. Customers and other parties (such as suppliers) can also initiate legal action when they're affected by an organization's non-

compliance with guidelines for security — especially the protection of personal information. Think of a healthcare provider, for instance, violating HIPAA regulations by sharing a patient's information without permission.

At worst, when a business repeatedly violates applicable regulatory requirements for cybersecurity, it can fall under a regulator's constant watch. Trends of compliance violations serve as a red flag to regulatory agencies, and a business can be reprimanded accordingly.

The Benefits of Compliance

- **Enhanced data protection.** Compliance verifies your business has taken appropriate measures to protect sensitive data and prevent data breaches.
- **Improved customer trust.** Demonstrate your ongoing commitment to protecting customers' data and privacy to bolster their trust.
- **Greater legal protection.** Gain additional legal protection and insurance coverage to limit potential liabilities in the event of an attack or data breach.

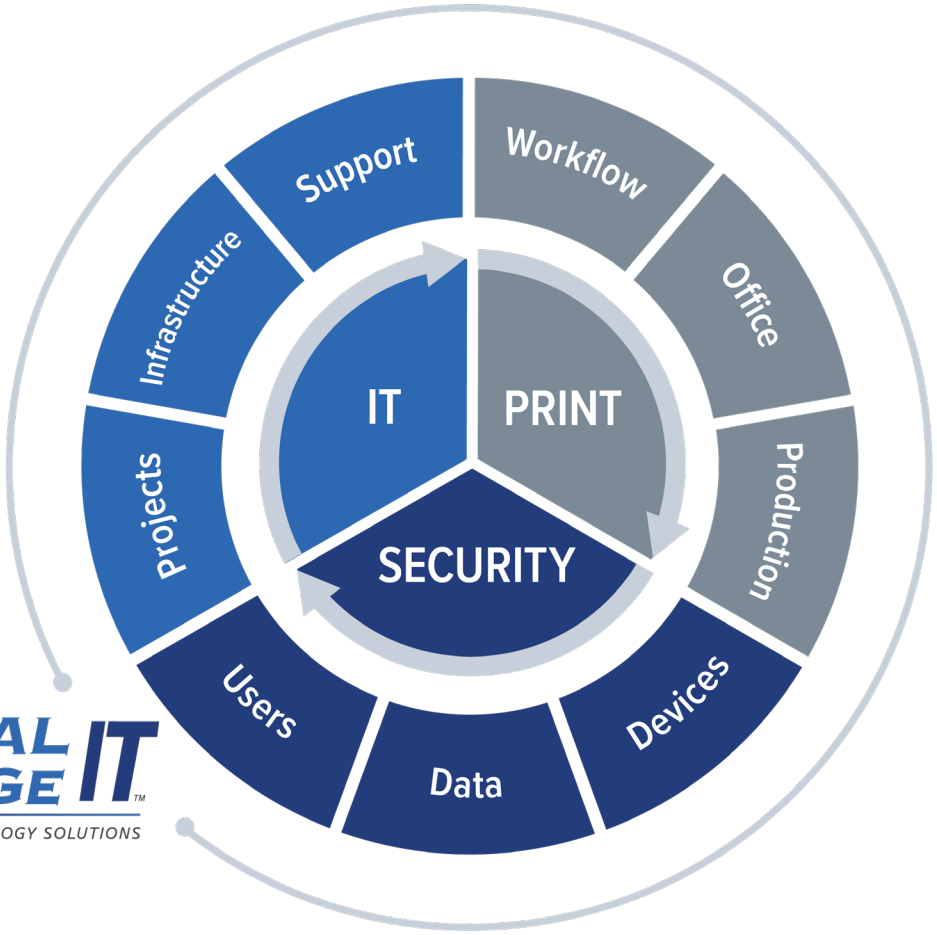
Conclusion

Businesses today face cyber threats of increasing sophistication, frequency, and volume, magnified by cybercriminals turning to emerging technologies like AI and even Ransomware as a Service (RaaS). For virtually any business, a single breach or attack can lead to operational disruptions and significant financial losses, along with reputational harm and the loss of customers' trust. This makes cyber insurance a far more vital component of any cybersecurity and risk management strategy, offering both financial and reputational protection against cyber-related incidents.

By understanding the increasing importance of cyber insurance coverage, assessing and managing organizational risks, and implementing strong cybersecurity measures, a business can enhance its resilience against cyber threats and ensure business continuity in the face of potential cyber incidents.

About Us

Visual Edge IT is a technology services provider for over 45,000 businesses, schools and universities, religious organizations, and local governments across the United States. We help organizations improve workflows, reduce costs, innovate, and secure their devices and data.



VISUAL EDGE IT™
SECURE TECHNOLOGY SOLUTIONS

- Managed Security
- Managed IT Services
- Managed Print Services
- Cloud/AI
- Communication & Collaboration
- Printer & Copier Services

About Visual Edge IT™, Inc.

Visual Edge IT, Inc. (VEIT) specializes in managed IT services, security, cloud computing, and print/copy solutions. Visual Edge IT™ is backed by more than 20 years of technology knowhow and a national network of expert engineers. The company is headquartered in North Canton, OH, USA. For more information, visit www.visualedgeit.com.