Cyber Resiliency and Risk Mitigation

VANTAGE

September 2022 | Interview

23 min read

Vantage cyber and information security experts weigh in on the impact of cyber resiliency and risk mitigation protocols on securing cyber insurance protection and minimizing business risks.

Malware, ransomware, and phishing attacks are rising, and no industry, company, or individual is immune. In 2020, there was a new attack on the web every 39 seconds with 63% of the data breaches being financially motivated. Today, malicious payloads distributed via email are responsible for 91% of all cyber-attacks. Despite the heightened and growing risk of cyber catastrophes, 62% of global organizations cannot claim that they are equipped to handle a cyber-attack. Public and private sectors are not aligned on safeguards, processes, or standards. If this unsustainable trajectory continues, according to data from Cybercrime Magazine, by 2025 global cybercrime damage is predicted to hit $10.5 trillion (about $32,000 per person in the United States) annually.

Businesses must stop treating cyber-attack as a black-swan event. Preparation and continued training regarding standards and best practices can cut down reaction time, lower risk, and eliminate recurring training investment every time an incident occurs.

Taking steps to analyze and understand where weaknesses exist and taking measures to reduce these exposures for cyber-crime is critical. If organizations are not prepared and rely on a reactionary approach, then it is often too late and very costly.

Insurers are in a unique position to help insureds better understand cyber risk exposures and push for the adoption of best-in-class cyber-hygiene practices. The adoption of more resilient online behaviors helps to mitigate loss potential. It also promotes a more sustainable cyber insurance market that functions to efficiently reduce and transfer risk.

Cyber Resiliency and Risk Mitigation

VANTAGE

Farhan Shah is Chief Technology & Information Security Officer at Vantage

Q. From a general business management perspective, how important is cyber resiliency and having solid practices in place to protect against cyber risks?

Whether buying insurance protection or not, there is a lot to be gained and much loss to be avoided by adopting and adhering to firm policies and procedures around a risk-based approach to cyber practice. While cyber insurance can mitigate the financial impact associated with cyber incidents, the potential operational or reputational impacts from a cyber event are better mitigated through solid practices and a robust control environment to lessen the likelihood of occurrence. **No company is completely immune to cyber breaches,** but with the right talent, tools, policies, procedures and training, companies can significantly heighten security levels and reduce the potential loss that could be experienced following a cyber event.

Q. Are there some easy things company leadership can do to improve resilience and reduce exposure to cyber threats?

Yes, there are a number of things that can help, including:

Data inventory and protection
Knowing what data an organization has, where it is stored and how it is used is a key element toward protecting the most critical data within an organization. Data can then be classified and appropriate controls can be implemented to help ensure that sensitive data is identified and protected appropriately.

Identity access management and role-based access
Assigning access permissions based on an individual's applicable role or job function aids in the access recertification processes and helps to ensure the principle of least privilege.

Patching hygiene
Applying patches in a timely manner is key to ensuring that technology assets are not subject to known vulnerabilities.

Physical security of data centers, offices etc.
Providing suitable security controls over office environments and

physical infrastructure is important to prevent adverse impacts to the confidentiality or availability of information assets as well as to protect employees present at such locations.

Third party risk management and follow-up

Assessing the risks associated with third party business relationships and periodically revisiting such assessments is an important element of risk management, particularly for any third-party relationships that involve the processing of sensitive information.

Incident response and crisis management

Robust incident response procedures, including clear escalation methods, are essential to ensuring that unforeseen incidents are remediated effectively and efficiently and communicated to relevant stakeholders. Conducting Tabletop exercises (a way of evaluating an organization's incident response plan) helps to equip and prepare incident response teams. And, it is critical to ensure alignment with external breach partners on a regular basis.

Threat intelligence and external news management

Remaining apprised of emerging threats and related sources of intelligence is a valuable means of staying ahead of potential exploits and proactively avoiding possible adverse impacts.

End-user security awareness training

Training all users in effective cyber hygiene and best practices helps to establish defense-in-depth protections against common threat vectors, including phishing.

Air-gapping back-ups

Maintaining copies of backed up data that are inaccessible from production operating environments helps to minimize the impact of any potential successful ransomware attack.

Q. What are the most significant challenges to good cyber hygiene and resilience?

Three main challenges come to mind as the most significant:

The cyber-security poverty line

For small to mid-size companies, there may be budgetary challenges limiting the establishment of robust cybersecurity protections. While this primarily impacts the entity with the budgetary constraints, there can be collateral impact throughout the remainder of the industry.

Cyber Resiliency and Risk Mitigation

Supply-chain related risks and potential lateral impact through data sharing or system connectivity across an established business relationship mean that risks faced by budget-strapped entities are not necessarily limited to their own environment. This challenge further accentuates the importance of robust third-party risk management practices.

Cloud – Zero to Verified trust for workload

Zero Trust has become a standard for securing a remote workforce. Zero trust works off the principle that you cannot inherently or blindly trust anyone, including employees, and you should only allow people to access the systems and applications they need to, when they need to (ex. working hours), in the way they should (ex. from a company asset). Additionally, enhanced authentication to verify who they are, authorization if they are accessing a company resource, and accounting for or tracking this access are the biggest keys to zero trust. Overall, this will ensure people have access to the least number of systems for the least amount of time, with the least level of permissions to successfully do their job.

Cyber hygiene

Cyber-hygiene examines the health, stability, and security of our systems starting with comprehensive education and continued training.

The next generation of computer engineers, programmers, and technicians will be relied upon to have the education and training to hold cybersecurity jobs that safeguard and protect businesses. It is also the responsibility of every employee to know what to look for and how to avoid taking accidental risks or falling prey to malicious attacks. This requires a commitment to establishing ongoing cybersecurity training programs for employees, and ongoing testing to verify that the training is effective. Security practices must accelerate as technology evolves and infiltrates every aspect of our lives. With this in place, the impact of attempted cyber-attacks can be greatly reduced.

Q. What are some best practices for analyzing the security of third-party service providers or business partners?

Analyzing the security posture and maturity of third parties requires a careful analysis of various elements of the entity's information security practices and related control environment, taking into account what type of data and information the vendor will store or have access to.

For organizations that have a completed independent attestation such as

a SOC 2 Type II, such documentation can be obtained and reviewed as a valuable independent analysis of the organization's control environment. Organizations may also consider requiring potential business partners to complete due diligence questionnaire (DDQ). Responses to the questionnaire can then be analyzed for suitability of the cybersecurity protections in place at that organization. When warranted, follow-up discussions are commonly held to obtain more clarity over DDQ responses. Organizations that maintain their own Standardized Information Gathering (SIG) questionnaire have the opportunity to provide that documentation as additional support.

Andy Lea is Senior Vice President of Cyber, Tech, MPL, Media Insurance at Vantage

Q. What are the top 10 network security controls Cyber underwriters expect to see?

There is much more consistency today around the basic level of expectations underwriters expect to see when evaluating clients' risk levels. While there will be some differentiation, and while there are a host of other factors considered throughout the underwriting process, at the most basic level the following network security controls are expected to be in place if insurance protection is to be offered:

Comprehensive Multi-factor Authentication (MFA) plus Strong Password Controls:
For many cyber underwriters, this is the most important control. According to figures cited by the United States national security cyber chief, between 80-90% of cyber-attacks could have been prevented using MFA. Multi-factor Authentication and strong password controls protect an organization against phishing, social engineering and password brute-force attacks and help prevent logins from attackers exploiting weak or stolen credentials.

Cyber Resiliency and Risk Mitigation

Network Segregation and Network Segmentation:

Network Segregation (separation of critical networks from the internet) and Network Segmentation (splitting larger networks into smaller segments) help reduce the risk and potential impact of ransomware attacks and will improve IT professionals' auditing and alerting capabilities, which will assist in identifying cyber threats and responding to them.

Strong Data Backup Strategy:

A strong data backup strategy is typically part of a solid Disaster Recovery/Business Continuity Plan. Underwriters want to see daily data backups, backups stored in more than one location, access rights limited to data backups, etc.

Disabled Administrative Privileges on Endpoints:

Disabling administrative privileges on endpoints improves security posture. An administrative end-user on an endpoint for even a few minutes can lead to catastrophic data breaches if the endpoint is compromised.

Security Awareness Training for Employees:

Security awareness has never been more important. The threat environment is evolving rapidly. Regular and frequent employee training is a must in today's environment.

Endpoint Detection and Response (EDR) and Anti-Malware:

Underwriters look for both EDR and Anti-Malware prevention tools. EDR provides advanced measures for detecting threats and provides the ability to identify the origin of an attack as well as how it is spreading. Anti-malware is a version of EDR that scans systems for known malware such as trojans, worms, and ransomware, and removes them upon detection.

Sender Policy Framework (SPF):

Underwriters look for this defensive tool, which plays an important role in email authentication. It helps prevent emails from unauthorized senders being received in employee inboxes.

24/7 Security Operation Center (SOC):

A dedicated SOC acts as the first line of defense against cyber threats, and cyber underwriters view this as a key proactive approach to network security. The analysis and threat hunting conducted by SOC teams help prevent attacks from occurring in the first place. SOCs provide increased visibility and control over security systems, enabling the organization to stay ahead of potential attackers.

Cyber Resiliency and Risk Mitigation

Security Information Event Management (SIEM) Platform:

SIEM tools collect and aggregate log and event data to help identify and track breaches. They are powerful systems that provide security professionals with insight into what is happening in their IT environment and help track relevant events that have happened in the past.

Strong Service Accounts Security in Active Directory:

Service accounts should be removed from Domain Administration groups. Assigning service accounts in built-in privileged groups, such as the local Administrators or Domain Administration groups, can be risky.

Q. Does good cyber resiliency help companies secure insurance coverage?

In today's cyber insurance marketplace, good controls are not only critical to getting favorable terms and conditions, they are critical to securing any cyber insurance coverage. Entities without basic controls like Multifactor Authentication (MFA), endpoint protection and response, and robust backups might not be eligible for cyber insurance.

Q. What other considerations are necessary for (i) larger clients with more complex risk profiles or (ii) small to mid-size clients?

Given the current threat landscape, both large and middle-market accounts need to adopt a holistic "defense in depth" approach to cyber security that promotes resiliency of networks and securing of critical data. This is becoming even more critical as the regulatory landscape also gets more complex with state after state passing their own privacy laws and data breach notification laws with very prescriptive breach notification requirements. All companies must know what data they are collecting, how they are protecting it. They must also know how to respond and how to notify individuals and law enforcement should a breach occur. Most importantly, they must know how to recover from a breach.

Q. Vantage is in the early stages of entry into the cyber insurance market. What are you seeing so far, and what insights do you have for companies seeking coverage?

Vantage began underwriting cyber insurance in 2022 and is providing much needed capacity and expertise initially to the large and complex risks that purchase large towers of cyber insurance. We pay close attention to the cyber hygiene of our clients as a strong indicator of insurability.

Cyber Resiliency and Risk Mitigation

The continuing increase in number and severity of cyber-attacks impacting companies emphasizes the growing need for protection against these risks. With a shortage of capacity for this protection, those companies offering coverage will be more and more selective with the risks they assume. Having critical controls in place will lead to a much better outcome for insurance purchasing. Insurance is playing a critical role in advancing cyber resiliency at companies large and small by requiring baseline standards of cyber defenses for insurability in the wake of significant increase in ambient exposures. As a technology and data enabled underwriting platform, Vantage is not only utilizing application information in the underwriting assessment around the adequacy of cyber defenses but is also ingesting curated digital security signals in the underwriting process. The team at Vantage is pleased to be bringing this much needed capacity to the marketplace. We are excited to see how this area of risk develops over time.

Alex Blanco is Chief Executive, Insurance at Vantage Group

Q. As an industry, are there additional steps could be taken to reduce cyber risks and improve protections against cyber-attacks?

Two opportunities come to mind

Centralized Standards and Data Sources

Creating a global governing body to implement standards and process could be a major step towards reducing risk and cyber-attacks across industries. The insurance industry has been able to identify risk patterns from external sources, such as the United States National Transportation Safety Board's commercial auto incident dataset. Similar progress could be made with cyber and infrastructure datasets, particularly as this data continues to grow. A centralized data source can not only identify trends and emerging risks, but also produce key learnings to inform training needs. The National Institute of Standards and Technology (NIST) and the Cybersecurity & Infrastructure Security Agency (CISA) lead the national effort in the United States to understand, manage, and reduce risk to its cyber and physical infrastructure. Partnering with these groups would bring credibility and vast expertise to creating and upholding security standards.

Cyber Resiliency and Risk Mitigation

Incentivize for Cybersecurity Prevention

Much like the auto and healthcare industries have required built-in safety standards, requirements, and incentives, the insurance community would benefit from doing the same. Requiring our insured companies to prioritize and elevate cybersecurity protocols could lead to significant reduction of risk. Adjusting premium rates for those clients who implement higher levels of cyber hygiene and are willing to report any holes in their systems would incentivize elevating these internal controls and practices for improved protection.

Q. After an abrupt shift in the cyber market in early 2021 in response to increasing frequency, severity and sophistication of cybercrime, what gives you confidence as Vantage builds its cyber business?

Cyber underwriters have introduced a great deal more rigor in their underwriting practices in reaction to the increased activity by bad actors, and there is greater alignment among insurers around a consistent set of network security controls that exemplify good cyber hygiene. That is good progress in what will be a long-term, evolving area of risk.

While we expect ongoing volatility and sophistication of cyber-crime, Vantage has the right talent and the right mindset to help our clients better understand their risks so greater protections can be put in place before a cyber-event has the opportunity to impact their business. I am confident that Andy and his team, with support from technology and security experts like Farhan, will leverage the best of their accumulated knowledge and experience to make smart risk decisions, and to support our clients in improving their risk profiles through these uncertain times.

Conclusion

As the frequency and intensity of cyber-attacks increases, vigilance and commitment to taking all measures necessary will be critical to mitigate their impacts. Now is the time to spread awareness, educate, create new standards, and set policies to protect our futures.

Cyber Resiliency and Risk Mitigation

About the Interviewees

Farhan Shah is Chief Technology & Information Security Officer at Vantage

Farhan is an experienced technologist with over 20 years in the technology and financial services industries working as a senior executive at Fortune 50 companies.

Andy Lea is Senior Vice President of Cyber, Tech, MPL, Media Insurance at Vantage

Andy has over 25 years of underwriting experience across cyber and many professional liability lines of business. Before joining Vantage, Andy lead underwriting for cyber, tech, mpl and media at CNA.

Alex Blanco is Chief Executive, Insurance at Vantage Group

Alex is a seasoned insurance professional with over 25 years of insurance expertise across Professional and Specialty lines of business. Before Vantage, he was Chief Underwriting Officer, Specialty Americas at AXA XL.

This interview was conducted by Laurie Orchard, Chief Operational Officer, Vantage Risk Ltd. and edited by John Flannery, Vantage's Interim Head of Marketing and Communications.

Cyber Resiliency and Risk Mitigation

VANTAGE

References:

1. How Many Cyber Attacks Happen Per Day in 2022? (techjury.net)

2. IBM Study: More Than Half of Organizations with Cybersecurity Incident Response Plans Fail to Test Them - Apr 11, 2019

3. Tech Execs: Multi-Factor Authentication Can Prevent 90% of Attacks - Infosecurity Magazine (infosecurity-magazine.com)

4. The cybersecurity jobs crisis is getting worse, and companies are making basic mistakes with hiring | ZDNet