Cyber Security & Business Interruption: Foundations for Prevention and Mitigation

By Jessica Eldridge and Ron J. Yearwood, Jr. of JS Held

Introduction

The modern security ecosystem is diverse and ever-changing, a place where cyber risk is top of mind for leaders at all levels, and threats to information / data security and privacy evolve at the speed of the technical innovations driving progress. Within this dynamic ecosystem, we are increasingly connected across the globe, where organizations and individuals equally face the ever-present threat from cyber-attack. No one is immune, the potential impact of a successful digital attack on your assets can affect operations, reputation, customer goodwill, and so much more.

Our data is increasingly under attack. Information is the life blood of our continuously evolving and increasingly connected global community. The power of data can be seen in all facets of the modern era, where the value of information has never been at a higher premium, giving rise to cutting-edge development and advancement. Unfortunately, as is often the case, the risk to the item of value increases at an equal or higher rate as that of the item's expansion. Information has become one of the world's most valuable intangible assets, while concurrently occupying the position of being one of the globe's most vulnerable assets. Inherent risk is an expected outcome of this transformative process, ushering in great responsibility to protect the information that drives our advancement.

This article focuses on the professional expertise, processes, and technologies that are needed to mitigate the ever-increasing risk of cyber-attacks and potential business interruptions on companies, organizations, and individuals.

The threat to information can be measured in many ways – from careless handling of data to the ongoing efforts of malicious actors to exploit, alter, or exfiltrate data. It is often the realized impact of this risk that ignites advancements in Cyber Security. This commodity we call information has transformed the way the world thinks and its place within the security function has become ever-present and ever important.

Considering this dynamic climate, addressing Cyber Security and business interruption impacts has never been more crucial for risk management and organizational success. Regardless of the size of your organization, a cyber-attack can be extremely costly and detrimental to your business's survival.

The heightened threat environment has made it imperative for organizations to maintain cyber insurance due to the growing sophistication of the threat actors. At the same time, cyber liability insurance coverage has become more expensive and harder to obtain. Premiums for these plans have been on the rise due to increased claims-related losses, rising demand for coverage, and large payout from ransomware attacks. Cyber insurance premiums increased by an average of 28% in the first quarter of 2022 compared with the fourth quarter of 2021. The evolution of the cyber insurance market has

seen a shift from blanket policies with broad inclusions and high limits to policies with detailed coverage, clear technical and security requirements, and managed limits based on claim trends.

The complex insurance landscape can be seen as one of several factors converging to create an environment that may be well situated for turbulent weather. Possible elements that could be included in the coming storm, are:

- Increasingly successful attacks on businesses of all sizes necessitating ransom payments,
- Filing of cyber insurance claims in record numbers,
- Growing losses from cyber incidents to include cyber insurance claims and growing civil litigation payouts,
- Increased focus from regulators and legislators on not only methods of prevention and response, but also the willingness of organizations to adequately invest in Cyber Security in advance of an attack, as seen in the recent Cyber Security recommendations from the U.S. Securities and Exchange Commission (SEC).

Understanding How to Combat the Cyber Threat Actor

While this current situation appears dire, never before have the tools and resources been available in the volume, comprehension, and variety to meet the challenge and reduce the risk.

As the threat from cyber-attacks has evolved, so have those who would challenge the apparent invincibility of the threat actors. They often seem to be one step ahead and better prepared. However, if we utilize the resources at our disposal in advance of the potential attack, we can effectively prepare and respond to minimize the impact of this perceivably unbeatable foe – the "Cyber Threat Actor."

To meet the growing challenge, Cyber Security professionals must leverage the people, processes, and technology at their disposal, to protect the confidentiality, integrity, and availability of the data / information they are responsible for; thus, ensuring security and privacy.

There are some foundational concepts that are critical to success.

> **Culture** is important. A top-down approach to addressing security within an organization is vital to achieving holistic participation. Cyber Security is a team event that requires everyone from the receptionist to the CEO to participate for the most effective results to be realized. If an appropriate culture of security and senior level engagement is not achieved, inspiring adoption of practices that create a good cyber culture can be challenging. Top level engagement is crucial and recent guidance from the SEC regarding better transparency at the board of directors level reinforces this foundational concept.
>
> **Planning and preparation** in advance of an incident are also critical components of an effective cyber security program. Given the growing business interruptions and breach-related losses, a strategy is needed to reduce risk of significant exposure. This concept becomes increasingly important in the effort to obtain cyber insurance that effectively covers the identified risk with appropriate limits. Unique to each organization, considerations include security and response strategy, incident response (IRP), business continuity (BCP), disaster recovery (DRP) strategies), policy / procedures, governance, pre-event financial recovery plan, and training. Efficient response to a cyber incident includes preparation for implementation of technical measures,

along with financial preparation and planning. Mitigating the potential financial impact of a breach includes understanding of financial impacts of a breach, insurance coverage and timelines, and internal issues including payroll and waiting periods, to name a few.

Identification of your organization's technology universe is often overlooked by security professionals. Areas of consideration should include asset inventory and mapping (hardware, software, and data for privacy including intangible assets such as business trade secrets and intellectual property), gap analysis, risk, and vulnerability management to include third party risk. Identification is not limited to technology. When evaluating an organization's critical data, consideration should be given to trade secrets which are legally protectable when they are secured via "Reasonable Measures." According to the U.S. District Court for the Northern District of New York "[i]n evaluating reasonable secrecy measures, courts look to whether . . . the information is guarded by physical- or cyber-security."[1] People and process elements to be considered may include critical document backups for human resource issues, payroll, as well as financial analysis to identify lost income, and eventually, incident mitigation expenses.

Protecting and defending the network includes elements such as awareness and training, patch management, access management, protective technology, and security operations. It is within this topic area we discuss the importance of layers of defense and that hygiene is not just for humans. Good cyber hygiene means utilizing software that scans for computer viruses and malware, installing network firewalls, changing passwords regularly, updating apps and operating systems on all devices on a regular basis, and much more.

Detection as a concept dictates that a strong defense is not enough. Well-prepared organizations are constantly on the lookout for anomalies through the use of logs, network scanning, event monitoring, and periodic exploit testing. It is important to keep in mind that monitoring for Cyber Security issues must provide a view from both the outside looking in (perimeter defense) and from the inside looking out.

Response to incidents requires a coordinated, well-planned, trained and practiced effort. Advance planning is critical to response. Practice of the plans at all levels solidifies the organization's ability to effectively respond with a proactive strategic focus. IRPs often include measures to contain, investigate, and eradicate threats, as well as identifying and eliminating root cause vulnerabilities while documenting evidence for various purposes. This information will also provide value in answering questions important to insurers who will need to gain a solid understanding of what happened and what the impacts were on operations physically and financially.

Recovery operations typically come later in the response effort but are critical, nonetheless. Backups are often the primary focus of the recovery discussion, but restoration of operations is often much more complex and can include the ongoing hunt for threat actors, additional security applications, and due diligence across the enterprise. Advance preparation in this category provides an organization the ability of clearly articulating costs to restore operations as

[1] *Executive Trim Construction, Inc. v. Gross*, 525 F.Supp.3d 357 (N.D.N.Y, 2021).

opposed to implementation of enhancements which will provide a trigger for insurer scrutiny and may impact your business income recovery.

Finally, applying **lessons learned** in order to improve affords an organization opportunity to leverage even the smallest of events to enhance response to future incidents

Conclusion

Aggregating these components into an effective Cyber Security program requires a proactive leader with vision who embraces collaboration. As noted, Cyber Security is a team sport that demands knowledge of industry best practices, the ability to establish the best compilation of services and capabilities for the organization to deliver the expected risk management posture, and the determination to follow through with the effort to full implementation.

The right information security / privacy leader is expected to empower, protect, and enable the enterprise, operations, and marketability, through delivery of the best available security operations program. If required as part of the enterprise, this leader will drive compliance including regulatory, legal, and governance programs, while inspiring a culture of security and initiative.

Resources necessary to fulfill this mission are not always available within the organization. Partnering with a service provider who can respond when needed to enhance capabilities is vital to the best of Cyber Security leaders. Some of the best service providers deliver tailored services to fill in the gaps where necessary. Organizations should look for providers that offer services that are individually customized for each client in their effort to establish or enhance their Cyber Security program. In the end, the best providers should supply a team of experts that bring decades of experience to each engagement, specializing in incident response and recovery, proactive resiliency building, pre-event financial planning, and financial loss analysis.

Acknowledgments

We would like to thank Jessica Eldridge, Ron J. Yearwood, Jr., and Robert McSorley for providing insight and expertise that greatly assisted this research.

More About J.S. Held's Contributors

Jessica Eldridge is a Vice President in J.S. Held's Forensic Accounting - Insurance practice. She has over 19 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 oversite of property damage claims for large construction projects.

Jessica can be reached at jeldridge@jsheld.com or +1 401-301-8565.

Ron J. Yearwood, Jr., CISSP, CISM, CIPM, is a Senior Managing Director who leads the Cybersecurity team within the Digital Investigations & Discovery division, a part of J.S. Held's Global Investigations practice. This includes Incident Response, Proactive Resiliency Services, Litigation Support, and Strategic Communications. Ron brings more than three decades of experience, including more than 23 years with the Federal Bureau of Investigation (FBI), where he led strategic and investigative operations against hundreds of criminal and nation state cyber threat actors. During his tenure in the FBI Cyber Division, Ron served as a representative to the White House Cyber Response Group. He is a certified information systems security professional, a critical incident stress management professional, and a certified information privacy manager.

Ron can be reached at ron.yearwood@jsheld.com or +1 904 375 7792.

Robert McSorley is a Managing Director in J.S. Held's Intellectual Property Practice. Based in the Chicago office of Ocean Tomo, a part of J.S. Held, Robert has 30 years of experience addressing the economic, financial, and accounting issues concerning commercial litigation. Robert has focused on intellectual property disputes since 1998, and regularly evaluates the measures and amounts of monetary recovery for infringement / misappropriation. He has offered expert testimony in federal courts and in depositions on dozens of occasions, and courts and juries have adopted his opinions and conclusions. A certified public accountant and a licensed attorney, Robert is a member of the Licensing Executive Society, the American Institute of Certified Public Accountants, and the Federal Circuit Bar Association.

Robert can be reached at robert.mcsorley@jsheld.com or +1 312 327 4412.