Vendor Risk Management

How to Confront Third-Party Cyber Risk in Your Supply Chain

SECURE HALO
SECURING THE ENTERPRISE

Leading Threat Vector

Third-Party Cyber Risk

In 2017, WannaCry, a ransomware capability released by ShadowBrokers to the general public and exploited by criminal elements, locked upwards of 200,000 computers in 150 countries across sectors to include hospitals, finance, and telecommunications. With that kind of damage, it's understandable most organizations focus cybersecurity efforts on firewalls, patches, and updates, though true enterprise security considers additional threat vectors such as insiders and third-party dependencies.

If your organization was prepared enough to already have defenses or patches in place, then WannaCry was just another news item. If not, you might have been operating at DEFCON 5.

What if your organization relied on a WannaCry victim to run your online payment or medical records systems? What if you had production halted by the sudden unavailability of a crucial component? What if instead of a flashy global malware variant, your vendor was victim to a quieter attacker, perhaps slowly acquiring your intellectual property, client personal information, or using your networks as an additional pivot point to some other partner?

This is the hidden menace in today's digital ecosystem.

SECURE HALO
SECURING THE ENTERPRISE

Increased Interdependency: Essential to Compete

"No man is an island" is a quote dating back to at least 1624. Today, the same holds true for essentially any organization. At the local level, organizations are dependent on their employees to serve and protect them. As organizations grow, they will necessarily find avenues to reduce cost and increase efficiencies by outsourcing certain expertise—whether that be network managed services or security, manufacturing sub-components, points-of-sale, transport, or basic utilities. Today, all of these vectors can double as points of entry into your organization.

Should a bad actor gain access, they may find proprietary information about supply chain functions such as distribution and inventory management, as well as marketing strategies, sales information, intellectual property, and even security configurations. Indeed, there is a growing shift from physical security controls to digital controls in the supply chain, says Chris Adderton, Vice President of the Council of Supply Chain Management Professionals (CSCMP). "For example, where we used to have individuals responsible for physically checking the security of systems, we now see the rapid implementation of smart technologies and sensors. On the positive side, this enables companies to shift from being reactive to problems to proactive and preventative," says Adderton. "At the same time, these technologies introduce new and complex security risks that supply chain professionals must be aware of."

As the risk environment expands, Adderton urges companies to consider whether organizational change is required to elevate supply chain issues and professionals to the C-suite, traditionally the domain of finance, marketing, and IT. The National Institute of Standards and Technology (NIST) recognizes the enterprise nature of risk driven by the modern business digital ecosystem. "Cybersecurity in the supply chain cannot be viewed as an IT problem only. Cyber supply chain risks touch sourcing, vendor management, supply chain continuity and quality, transportation security and many other functions across the enterprise and require a coordinated effort to address," according to NIST's Best Practices in Cyber Supply Chain Management.

Key Cyber Supply Chain Risks

- Third-party service providers or vendors with physical or virtual access to information systems, software code, or IP.
- Poor information security practices by lower-tier suppliers.
- Compromised software or hardware purchased from suppliers.
- Software security vulnerabilities in supply chain management or supplier systems.
- Counterfeit hardware or hardware with embedded malware.
- Third-party data storage or data aggregators

SOURCE: NIST Best Practices in Cyber Supply Chain Management

A holistic approach to security is necessary to keep pace with—and hopefully get ahead of—a threat vector that isn't going away.

Third-Party Cyber Risk Outpaces Action

The number of data breaches and cyber attacks related to third parties continues to grow. In a 2016 Ponemon survey of 598 individuals across multiple industries, 73 percent of respondents said the number of cybersecurity incidents involving vendors is increasing. Almost half (49 percent) confirmed their organization experienced a data breach caused by one of their vendors but well over half (58 percent) said they're not able to determine if vendors' safeguards and security policies are sufficient to prevent a data breach.

67%

do not have or are unsure if their company has an inventory of all third-party vendors

SOURCE: BuckleySandler/ Treliant Risk Advisors

18%

say their company assesses the cyber risks of third parties

SOURCE: Ponemon/ Shared Assessments

98%

do not consider third-party access a top priority in IT initiatives and budget allocation

SOURCE: Soha Systems

Regulators Now Demand Board-Level Attention

While vendor risk management is moving from the back burner to the front for supply chain and risk management professionals, boards have a noticeably lower level of engagement and understanding of cybersecurity risks to vendors than to their own business, according to the 2016 Vendor Risk Management Benchmark Study. Its message to boards:

- Breach of your data through a third party is your company's responsibility
- Contract language does not provide full protection
- Monitoring and risk measurement should be reported to the board

Regulators such as the Federal Financial Institutions Examination Council (FFIEC) and the Office of the Comptroller of the Currency (OCC) now evaluate whether a board appropriately oversees the risks involved in its outsourced relationships. Whether vendor risk management is centered under compliance, information, or risk management functions, the OCC notes that "the board is responsible for overseeing the development of an effective third-party risk management process commensurate with the level of risk and complexity of the third-party relationships. Periodic board reporting is essential to ensure that board responsibilities are fulfilled."

What Regulators Look For

Due diligence of third party selection

Independent reviews

Ongoing monitoring

Documentation and reporting

SOURCE: OCC bulletin 2013

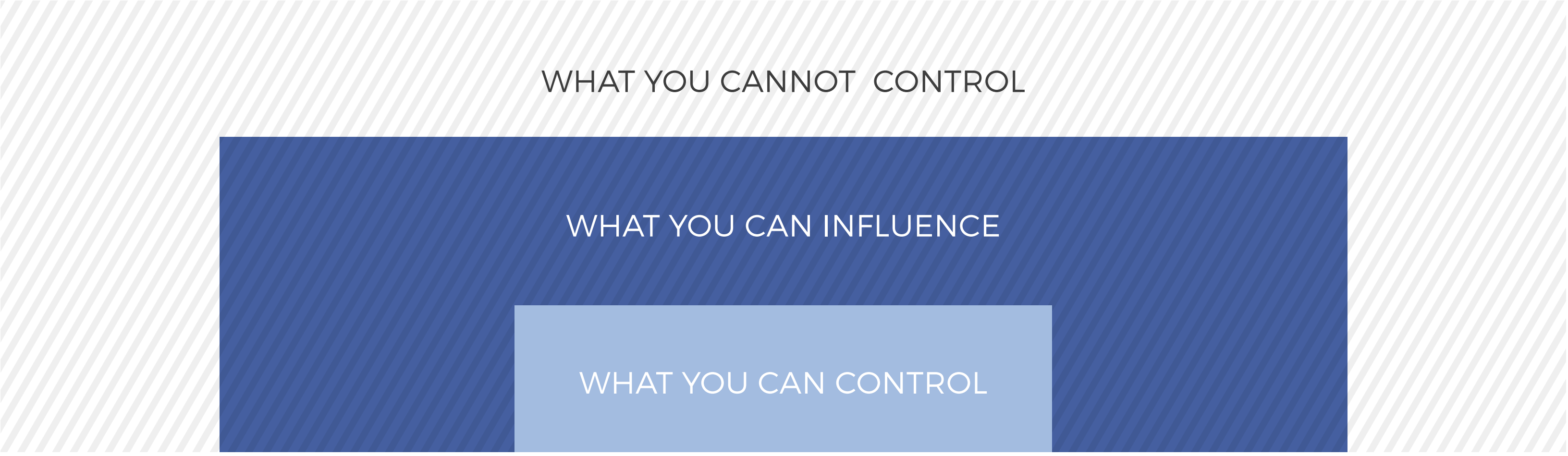
Regulatory Bodies

NY DFS | PCI 3.0 | HIPAA
OCC | CFPB | FFIEC
Federal Reserve | CFPB

A 3-Part Framework
for Viewing Risk

As the infrastructure we rely upon continues to become more diverse and our core business functions become decentralized in the drive to improve efficiency, it's necessary to adjust the optic through which we understand and manage cybersecurity risk. With critical dependencies expanding beyond the sphere of our control, we must posture ourselves in a way that allows us to minimize both our susceptibility to and the impact of cyber threats.

This, combined with expanding footprints outside the walls of an organization and the dynamic nature of the threat environment, has led Secure Halo™ to view cybersecurity risk through a three-part framework:



WHAT YOU CANNOT CONTROL

WHAT YOU CAN INFLUENCE

WHAT YOU CAN CONTROL

Areas that are managed as an extension of day-to-day business and the interfaces that extend outside the walls of an organization are those that can be influenced. For example:

- organizational processes for vendor management
- assessment of risk involved with outsourcing services
- articulation of language included in third-party agreements and contracts

> “If critical business functions are being outsourced, they become a single point of failure in determining your effectiveness. This makes applying a security process and security fundamentals to areas that are beyond your control, but not beyond your influence, essential to empowering your organization.”
>
> – Nick Streaker, Vice President, Technology, Secure Halo™

Although the services and products themselves fall outside of what your organization has direct control over, you do have the ability—and the responsibility—to shape the security environment in a manner that protects your organization from risk.

Third-party cyber risks should in fact be considered upfront when contemplating shifting the operational control of a critical element of the business, since doing so means you will relinquish some of your own preventative and detective control.

By identifying aspects of third parties’ security posture that align with or are in conflict with your own organization’s security, you shift from viewing third parties as a potential vulnerability, to recognizing them as an active participant in the improvement of your security posture and lowering your potential risk across the enterprise.

Ask Vendors
These Questions

1. Do you use multi-factor authentication?

2. What kinds of legacy defenses do you have in place, such as firewalls, anti-virus, and intrusion detection & prevention?

3. What encryption standards do you require for both data in transit and data at rest?

4. Has there ever been a significant cyber breach in the past?

5. If so, what was the cause and are there recovery time objectives?

6. What resilience measures are in place to prevent similar events from happening again?

7. How do you vet new hires? Upon termination, what protocols are enacted to ensure access paths and credentials are revoked?

8. Who and how many employees will have access to my data?

9. What types of preventative and detective physical security controls are implemented at this location, such as barriers, alarms, cameras, and intrusion detection?

10. To what extent is auditing performed on my account if changes are made?

Before You Move to the Cloud

Even while companies admit that they are not managing third-party cyber risk, the use of vendors continues to expand significantly. Gartner predicts a continued move away from Legacy IT services to cloud-based services, forecasting an 18 percent increase in the worldwide public cloud services market in 2017.

Secure Halo™ believes the best defense is a good offense—get ahead of risks with mitigating or preventative measures.

Take These Steps Before Outsourcing

1. Outsource only what is necessary. For example, don't sign up for complete managed services if cloud storage is all that's necessary.
2. Maintain primary control over who has access, and at what level, to network systems (especially production systems).
3. Ensure there is an independent capability to monitor and audit activities that is not simply a function of the provided solution.
4. Insist on full compliance when procedures and requirements must change.
5. Perform a careful legal, operational and technical review of contract terms.
6. Always check your cyber insurance policy for sub-limits and exclusions that preclude coverage for losses as a result of third-party disruptions.
7. Get your own house in order first. Ensure that Physical, Internal and Operational security controls are in place to secure data that may be accessed by external vendors.
8. Educate employees on third-party cyber risk.

While intelligent outsourcing can provide value to your organization, choosing the wrong provider can be devastating, which is why performing due diligence ahead of time is an essential part of the outsourcing process.

SECURE HALO
SECURING THE ENTERPRISE

Secure Halo™
Helps Mitigate Third-Party Risk

Adversaries are always looking for the path of least resistance, and that can often include use of third-party vendors and supply chain partners to gain a foothold into your network. The maturity of your security posture is meaningless if those connected to your digital ecosystem have exploitable vulnerabilities. Research by Ponemon has shown that many companies do not know how many third parties have access to their confidential information or whether those vendors are sharing the data with others. Ponemon also found that companies rely upon contractual agreements instead of audits and assessments to evaluate the security and privacy practices of third parties.

Secure Halo™ knows vendor risk management is complex, but we feel it shouldn't be hard. We created Secure Halo™ to simplify how you manage your digital ecosystem with a platform that is objective, repeatable, and scalable. Secure Halo™ offers in-depth analysis of a single organization or aggregated risk across a portfolio of partners or vendors. It's simple to share Secure Halo™ to understand whether third parties are managing security risks around people, processes, and technology.

Your C-suite will appreciate the executive summary and prioritized recommendations generated upon completion of an assessment, while your security and risk management teams will be able to drill down into results across six domains. With a dashboard of data and trends, it's easier to set security standards and spot outliers.

About Secure Halo™

Companies need meaningful insight into how vulnerable they are to expanding and evolving digital risks. Secure Halo™ provides enterprise cyber risk assessments, managed services, and cybersecurity consulting to Fortune 500 companies and federal agencies. Our Secure Halo™ platform provides a holistic view of cyber risk to empower market-driven and threat-based decisions, while also meeting regulatory requirements.

Learn more at www.securehalo.com