Cylitic Security

WHITEPAPER | SUMMER 2022

Third-Party Security, First-Priority Responsibility:

Solving the Challenge of Partnership Risk

TABLE OF

Contents

CYLITIC SECURITY

Executive Summary

THE PERFECT STORM OF THIRD-PARTY SECURITY RISK

Third-party cyber risk management is a growing and evolving challenge and presents unprecedented risks to both enterprises and their third-party partners. These risks are often difficult to quantify or assess, due to the sheer quantity of third-party partners connecting to the enterprise – the number of vendors an average enterprise supports continues to grow, in both number and degree of access to the enterprise.

These small partners create risk that is relatively significant compared to their size. And because these partners often don't have the resources to implement optimal security technology, nor hire sufficient dedicated security talent, there is often a lack of visibility into the true risks they pose to the enterprise. Compounding the scope of risk, small partners also typically have inadequate risk posture, a lack of consistent patch updates, and no effective means to continuously monitor risk indicators.

Malicious actors have taken notice – many adversaries target small companies as a first point of entry to compromise enterprises, knowing that their security posture is ripe for exploitation. Because enterprises cannot fully outsource security risk, there is additional scrutiny on the enterprise's leadership from corporate boards, and in extreme cases, has led to the termination of top executives, including CIOs and CEOs.

54%

Of senior security executives lack understanding of the levels of network access third parties have

65%

Don't know which third parties have access to their most sensitive data

74%

Of reported breaches are attributable to a third-party partner

182

Average number of vendors that connect to an enterprise organization's infrastructure each week

**Source: Ponemon Institute survey of security executives*

There are several pervasive aspects of enterprise and third-party preparedness that contribute to this challenge:

- **Lack of visibility into key indicators of security risk**
- **Low-quality and less robust security solutions**
- **Lack of resources committed to security**
- **Post-breach management is an ordeal**

Enterprise environments and third-party security are interdependent, commingled and interwoven. But organizations can effectively manage security risk by employing three mutually reinforcing and interdependent strategies to simplify security:

THE SELF-REINFORCING MODEL OF THIRD-PARTY SECURITY

1

Limit and control the data that is supplied to third party partners.

A first line of defense, continually adjusting and exerting control over the types and volume of data that are shared allows organizations to implement "dynamic" regulation of third parties and "throttle" data access, giving broader access to some and less to others as their risk posture changes over time.

2

Promote and enforce more robust security tooling requirements for third parties.

While technology alone won't solve an organization's problems, a robust infrastructure of security tools, in tandem with open channels of communication, can create the foundation for a responsive and continuous security posture.

3

Increase the signals of risk to Improve insights and dynamic decision-making capability.

Valuable indicators of risk include assessment of third-party partners' security posture: Are they FDE-enabled? Is there an active firewall? Are security patches up to date? Such indicators of poor security posture enable informed decisions on the level of access granted to these partners, and identifying anomalies and threats early increases proactive response capability.

INTRODUCTION

Challenges with Securing Third-Party Partners

In the domain of cybersecurity, it can appear that the only certainty is uncertainty. In particular, third-party cyber risk management is a growing challenge and opens opportunities for criminals to exploit an enterprise ecosystem's weak points to gain unauthorized access to critical applications. Unfortunately, the risks are not always easily quantifiable or proportionate: third-party relationships can create outsized risk relative to their security maturity and technical sophistication, particularly with smaller third parties (those with less than 50-100 employees). These small partners are often the first point of entry for adverse security events. And the endgame for malicious actors is often much more insidious – advanced adversaries often target small partners with the eventual goal of penetrating the enterprise.

Adversaries specifically target an enterprise's connected partners because, once breached, these partner networks serve as a launching point for subsequent attacks against the enterprise. These adversaries then exploit the partner's trusted access to pivot and gain access to enterprise internal networks, private applications, and sensitive data.

Meanwhile, the dependence on third parties for critical business functions continues to grow,[i] exacerbating the potential for catastrophe. This "perfect storm" of risk factors exposes enterprises to myriad risks, not least of which include significant economic impact, supply chain disruptions, major data breaches, and reputational damage. The fundamental truth at the heart of this conundrum is that enterprise security is increasingly dependent on the global security ecosystem, extending to its smallest partners.

This situation lays bare the reality that no matter how large an enterprise is, its security posture is reliant on all its stakeholders[ii] – including employees, contractors, suppliers, resellers, and cloud partners. Therefore, enterprise security is only as good as that of its weakest link. But currently, many organizations are woefully underprepared – in a recent Ponemon Institute survey of security executives, 54% of respondents admitted their organization lacks a sufficient understanding of the levels of network access third parties have, while 65% noted that they don't know which third parties have access to their most sensitive data.[iii] And perhaps unsurprisingly, 51% of organizations have already experienced a data breach caused by a third party – and in some industries, such as healthcare, this number rises to 80%.[iv] Of organizations that have experienced a breach, 74% noted that the culprit could be traced to access provided to third parties.[v] While a minority of organizations actually have the mechanisms in place to manage and confidently report on the status of their third party suppliers,[vi] the average organization has 182 vendors that connect to its systems each week,[vii] with a median total of over 5,000 third party contracts.[viii]

For details on recent prominent third-party breaches, see the Appendix at the bottom of this report.

Adverse Impacts to Enterprises

For enterprises, this means that without the right protocols and tools in place, a data breach is likely inevitable. And once a breach occurs, the economic impact and damage to reputation, systems, and operational workflow can be substantial – a recent estimate projects the total cost of third-party-related breaches to be between US$0.5 to $1 billion, or more (a figure that has more than doubled in the past 5 years).[ix] The implication of this potential for damage is that organizations that fail to take thoughtful steps to prevent, detect, and respond to third-party cyber incidents severely undermine their cybersecurity posture. Despite the increase in outsourcing and third-party services, enterprises will not be able to fully outsource cybersecurity risk – meaning that the full brunt of cybersecurity incident damage lies with the enterprise in the view of the public and their customers. This places additional scrutiny on the enterprise's leadership from corporate boards, and in extreme cases, has led to the termination of top executives, including CIOs, CISOs, and CEOs.[x]

Several aspects of both enterprise and third-party security preparedness contribute directly to this continued growth and damaging impact from security incidents, including:

01. Visibility

Lack of visibility into key indicators of security risk: Over half of enterprise organizations do not actively assess their third-party partners' security and privacy practices before granting them access to sensitive and confidential information – and these enterprises often vet suppliers based on reputation alone.[xi] Given the onslaught of recent high-profile enterprise breaches attributable to third parties, this lack of visibility and insight into the levels of risk that third parties present will only continue to increase in scale and scope if not urgently addressed.

02. Quality

Low-quality and less robust security solutions: The overuse of "homegrown" and free or consumer-grade products contributes substantially to breach risk. One in three companies with fewer than 50 FTEs is estimated to use free or consumer-grade products and budget 90% of their security spend on endpoint security.[xii] Security programs that rely on outdated and homegrown systems and manual processes create undue maintenance burden and increase the likelihood of human error. However, third parties' use of these substandard products is an unfortunate byproduct of limited spending capacity – smaller entities are often unable to access sophisticated tools from vendors who only target larger enterprises.

03. Resources

Lack of resources committed to security: Organizations are not taking the necessary steps to reduce third-party remote access risk, and thus expose their networks to security and non-compliance risks. As a result, 44% of organizations have experienced a breach within the last 12 months, with 74% saying it was the result of giving too much privileged access to third parties.[xiii] Because of their vulnerability, small businesses are three times more likely to be maliciously targeted versus enterprises.[xiv] Aggravating the challenge, smaller companies experience a lack of security talent due to the inability to afford necessary expertise.

04. Management

Post-breach management is an ordeal: A typical Incident response can take months and increase the likelihood of adverse impacts including dwell time for attackers and increased expenses through legal fees. This underscores the need to prevent security issues earlier in the process. Once an incident occurs, the organization must manage more technical debt, and even more security issues that must be dealt with, ultimately creating more expense.

Actions & Considerations

Although these challenges are substantial, they are certainly not insurmountable. Basic foundational actions can enable enterprises and third-party partners to stay in lockstep on security management. Two primary ways to achieve this are to (1) increase the real-time visibility of existing and potential cyber threats, and (2) implement responsive security capabilities that continuously detect, block and provide ability for analysts to remediate threats.

To address the concern of managing current threats, enterprises need better visibility into small partners' detection and response capabilities, along with the confidence to make informed decisions based on the insights gained. A solution to this challenge is to implement portals and dashboards that offer real-time visibility into small partners prevention, detection, and response capabilities. Portals and dashboards allow organizations to close communication gaps and create actionable insights that can drive organizational learning.

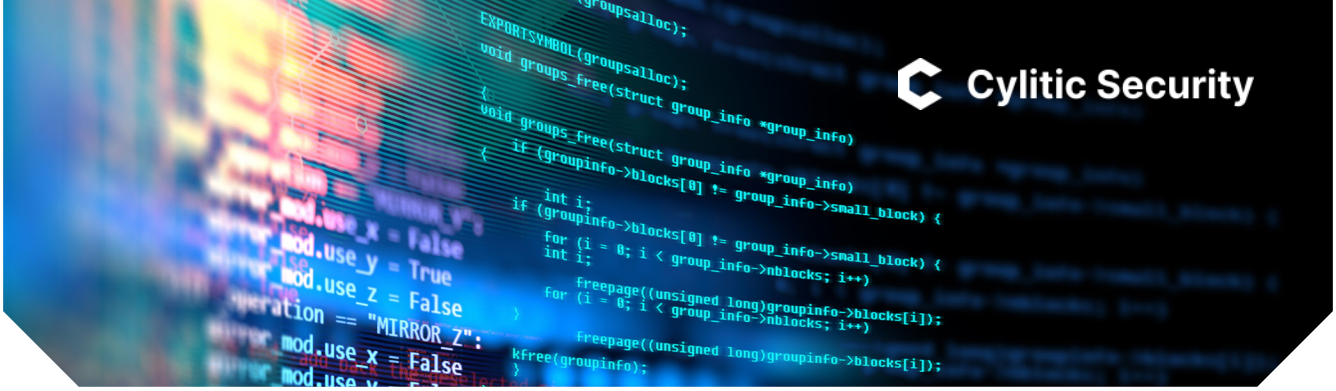
And to address emergent threats and maintain a continuous, responsive, and sustainable security posture, enterprises should embrace resilience, fluidity, and dynamic adaptive capabilities. Adaptive capabilities and continuous monitoring are necessary to adjust to evolving threat landscapes, while vulnerabilities and their remediation status must be consistently monitored among key stakeholders.

Monitoring and identifying threats, however, is only part of a comprehensive security program—the end goal is to materially reduce risks. Beyond enhancing visibility into third parties' detection and response capabilities, a managed security service to improve risk posture and remediate threats is critical to advance and sustain continuous cybersecurity readiness.

These actions and capabilities enable simplified, strategic, holistic, and continuous security management

As operations grow more complex, so do the number and nature of partners embedded in organizations' ecosystems. This means, in essence, that enterprise environments and third-party security measures are commingled and interwoven. But organizations can effectively address this challenge using three mutually reinforcing and interdependent strategies to simplify security.

Exhibit 1: The Self-reinforcing model of third-party security risk management



STRATEGY #1

Limit the Data Supplied to Third Parties

A higher volume of data points creates more attack surfaces and access points for malware and exploits. This potential is evident in reality: Organizations that have experienced a security incident also tend to share a higher percentage of their critical data than those who haven't been breached; and firms that have experienced an incident are less likely to have tools in place to mitigate third-party cyber risks.[xv]

As a first line of defense, continually adjusting and exerting control over the types and volume of data that are shared can go a long way toward keeping the enterprise secure. The ability to consistently adjust the amount of data access provided to partners is derived directly from access to insights – continual monitoring of the indicators of risk allows organizations to implement "dynamic" regulation of third parties and "throttle" data access, giving broader access to some and less to others as their risk posture changes over time.

KEY CONSIDERATIONS:

Restricted Access

The ideal goal is to move toward "least privilege" – access should be restricted to the least amount needed for a user to perform their role. Also, as much as possible, vendor access should adhere to a just-in-time model, meaning it is provisioned only when certain contextual parameters are met, and it is removed when the work is complete, the context changes, or after a certain amount of time has elapsed. No access should be open-ended and persistent. This approach enables the enterprise to dynamically suspend data access if endpoints do not meet established security posture thresholds.

Access Identification

Identify precisely which outside entities have access to what information. The inventory should include a data classification exercise, which involves categorizing data shared with third parties according to importance and sensitivity and determining the level of security required for vendors in possession of data in each category.

Tools & Preventive Measures

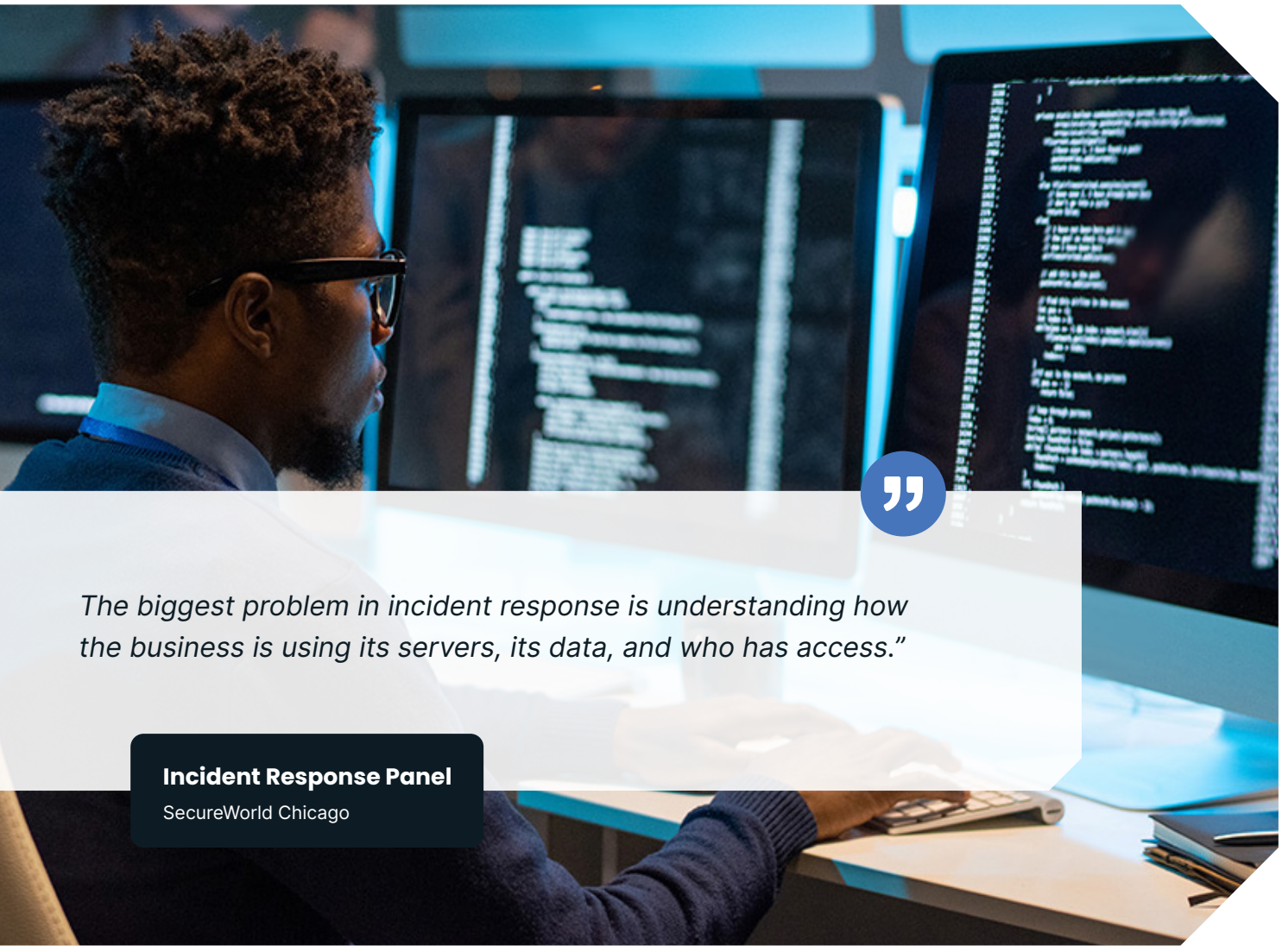
By employing security tooling, preventative measures, and maintaining a steady cadence of security risk signals, enterprises can continually adjust and dynamically control the risks related to information that is shared with third parties.

STRATEGY #2

Promote and Enforce Robust Security Tooling Requirements

As organizations move toward a model that incorporates a continual cycle of preventing, detecting, and responding to security issues, the right technology stack can enable and support efforts to create a comprehensive view of risks. As threats evolve at an increasing rate, solutions that automate processes and tasks, such as those incorporating artificial intelligence (AI) and machine learning can enhance business efficiencies and permit today's cyber workforce to proactively (and rapidly) address sophisticated cyber threats.[xvi]

And while technology alone won't solve an organization's problems, a robust infrastructure of security tools, in tandem with competent and skilled security analysts and open channels of communication, can create the foundation for a responsive and continuous security posture. Automated and low-touch tools can provide guidance on where to focus mitigation efforts and provide clearer context on the root cause of security concerns, before they become massive problems.



> *The biggest problem in incident response is understanding how the business is using its servers, its data, and who has access."*
>
> **Incident Response Panel**
> SecureWorld Chicago

COMMON TOOLS THAT HELP ADDRESS THIS INCLUDE

Endpoint Detection & Response

Endpoint detection and response (EDR) products allow the organization to continually detect suspicious activity and should confer the ability to respond in real-time to visualize the incident and make taking the appropriate action seamless.

Endpoint Encryption

Endpoint encryption reduces the burden of lost and stolen devices (a leading cause of breaches in industries such as healthcare and financial services).

Endpoint Vulnerability Management

Because user systems with security vulnerabilities are a prime attack vector, it is important to automate vulnerability scans and patch and remediation tools. Endpoints should be continually scanned for vulnerabilities and patched regularly to reduce risk. Daily scans of all endpoints, coupled with a mechanism such as a portal or dashboard to share key insights with the partner and the enterprise, are ideal.

Malware Protection

Malware protection (Next-Generation Antivirus, or NGAV). NGAV can proactively prevent and block malware and malicious attacks, even those currently unknown, by monitoring and responding to tactics, techniques and procedures (TTPs). The solutions employ predictive analytics enabled by machine learning and artificial intelligence to enhance threat intelligence efforts.

Web Filtering

Websites are the second most common malware mechanism. Therefore, it is imperative to universally protect your users from connecting to malicious websites or systems, and protect users, wherever they are. Security software employed should ideally proactively and automatically block phishing links to reduce the tendency for human error.

Automated Asset Discovery

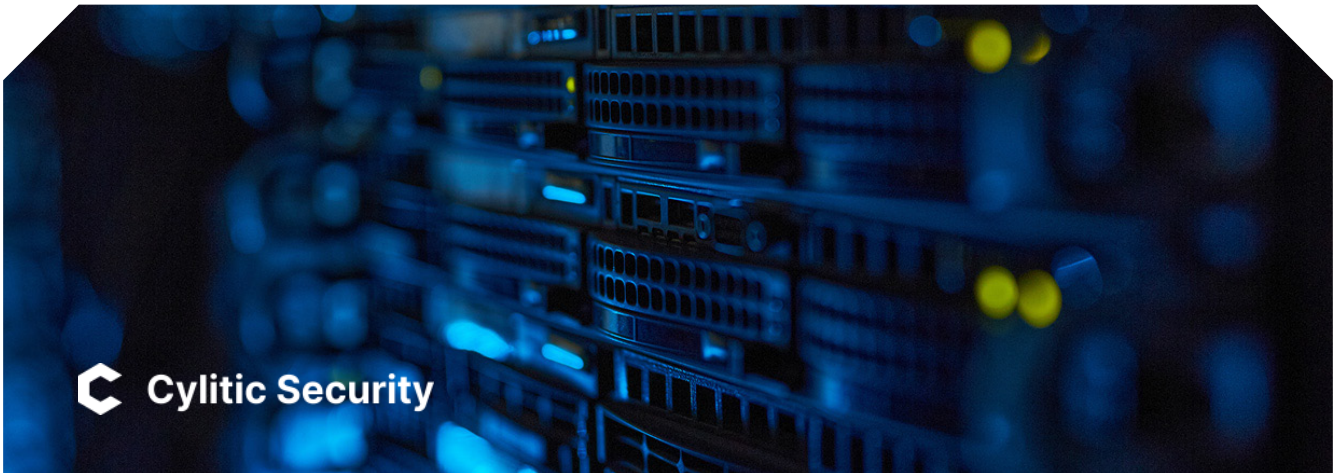
As the number of third-party providers inevitably changes over time (as new partners are onboarded), it is necessary to seamlessly ensure that operational continuity and reliability are maintained. Ongoing asset discovery also helps also to perform necessary vulnerability assessments to optimize risk reduction.

Email Protection

Email is a top attack vector for phishing and malware attacks such as ransomware (almost 3 out of 4 organizations in the United States have succumbed to a ransomware attack),[xvii] due to the nature of email anonymity, its versatility, and a high chance of success and ability to give attackers direct access to corporate networks. In many cases, attackers design their ransomware specifically to bypass traditional web and email protection.[xviii]

Threat Hunting

Threat hunting is defined as "The process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions."[xix] An optimal threat hunting solution generates alerts automatically and can apply insights from one instance to other users once discovered, creating higher returns on efforts.



STRATEGY #3

Increase the Signals of Security Risk to Promote Insights and Organizational Learning

Although the primary goal of organizations should be to prevent security compromise, there should be a continuous strategy to mitigate or at least minimize loss due to security incidents. Organizations must ideally identify threats, attacks, and compromises early, while they still fall in the category of “potential” rather than active or successful.

This will entail a discovery process to identify anomalies, in contrast to a baseline of usual communications in the environment where possible to make it easier to spot deviations. Once the baseline is established, continuous monitoring with embedded AI and ML characteristics that adapt to emerging threats, along with transparent and open communication channels are important to enhance alignment and decision-making capability.

Increasing the signals of risk also enhances the ability to dynamically control the amount of data shared with partners — if a partner is not FDE-enabled, is not firewall-enabled, and is out-of-date on security patches, they can be more easily categorized as deficient in security posture.

The Value of Portals to Capture Trends

Collecting and tracking security indicators accurately and consistently is critical to accumulate the data necessary to make informed decisions. However, this data in isolation has limited utility – making it accessible and insight-driven is a crucial next step. A portal can aggregate telemetry, alert, and incident information from disparate security systems and report it directly to decision-makers, simplifying compliance enforcement across the network and reducing gaps in communication.

A hallmark of a "gold standard" portal is the ability to visualize data and identify trends, providing powerful insight and transparency into key initiatives, and ultimately make an organization's operational processes and communications more efficient and effective.

KEY BENEFITS FROM USING A PORTAL TO CAPTURE SECURITY TRENDS:

- **Automated Certification**

  Automatically certify the security of your third-party partners' technological infrastructure and report that compliance status to them. Automated certification supplements the insights from time-consuming and often-unreliable risk assessment questionnaires and can increase decision-making confidence.

- **Partner Security**

  Ensure that all partners are secured and identify unmanaged systems. Portals allow users to drill into each view for more information, and can summarize problems and details on each partner system (are they FDE enabled, etc.)

- **Informed Decisions**

  Portals provide clearer context on what is contributing to problems, so that they can be mitigated early. Portals can be used to effectively display only the most useful and vital information, reducing confusion, and leading to smarter, data-driven decisions.

- **Data Reinforcement**

  Reduce the time to make intelligence-driven decisions and responses—mutually reinforcing your organization's data trust practices.

- **Progress Tracking**

  Seamlessly track progress and evolution of the security posture for third parties with real objective data obtained from security tooling versus simply "checking the box."

- **Contract Renewals**

  Actively control renewal of contracts based on changes in security posture for third parties and cease access for those firms whose risk posture does not meet the standard.

- **Security Management**

  More available indicators confer the ability to more fluidly make decisions on where and how to limit data sharing, as well as creates more data points that will help optimize forensic investigations and assess a more accurate state of security risk. However, enterprises must remain cognizant of balancing assessment of their tier-2 suppliers' cybersecurity posture, while not overburdening them with responsibility for security management that they may not have the capacity to support.

SUMMARY

Conclusion

Prevent, Detect, and Respond to Third-Party Cyber Risks

The cybersecurity function should be adaptable and efficient to adequately respond to increasing external threats and a growing talent gap from relationships with third parties to individuals performing the work.[xx] As cybersecurity threats evolve, adaptable approaches that automate critical processes are necessary, and can help enable even large international organizations to operate with the flexibility of a startup.

The ideal approach is one which connects decision-making capability, provides continual insight into areas of potential concern, and enhances organizations' ability to prevent more incidents, as well as respond more effectively to incidents once they occur. Seamlessly incorporating these actions into a cohesive and mutually responsive ecosystem help extend the range and effectiveness of threat visibility, coupled with a more-informed position upon which to base security decisions.

As the number of third-party connections grows, so do the risks of complexity, which has "driven cyber risks and costs to dangerous new heights."[xxi] The most basic of measures to curtail this complexity – reducing the number of vendors and third-party suppliers – is not always feasible or desirable. Therefore, an ideal approach is one that is automated, extendable, self-reinforcing, and enables visibility into key security indicators for third parties.

About

Cylitic Security

A fully managed security service and analytics platform for third-party risk reduction, Cylitic Security protects third parties, enables them to handle the risk of potential incidents, and provides an unprecedented level of visibility and analytics to the enterprise. Cylitic's mission is to quantify risk and enable clients to mitigate their company's exposure to cyber risk with top-tier protection, insurance, and automated security certification.

Collectively, the Cylitic team has successfully defended global Fortune companies and critical government systems and combines best-in-class Silicon Valley engineering with exceptional security talent to create the next generation of managed security services. Cylitic's people and technology work synergistically to protect their customers around the clock, and actively applies their skills and tools to help protect small mission critical companies.

Cylitic's low-code security automation provides a robust application development capability for use cases that can be solved with simple drag-and-drop data entry and business logic to extremely complex, sophisticated solutions that meet the needs of the entire organization. Cylitic's purpose is to bring advanced security capabilities and expertise to small to medium-sized customers who normally otherwise wouldn't have this access. Cylitic is leveling the playing field against threat adversaries who specifically target smaller organizations.

To learn more, visit cylitic.com.

Appendix: Prominent Third-party Security Incidents

ORGANIZATION	BREACH DETAILS
Home Depot	Home Depot was hit with a massive data breach that resulted in 56M exposed customer credit and debit cards.
Quest Diagnostics	12 million patients may have been impacted by a breach into American Medical Collection Agency (AMCA), the medical testing company's third-party billing provider. According to a data breach filing with the Security and Exchange Commission, as many as 11.9 million patients may have had their credit card, banking, medical information, and other personal details stolen.
Google	Immigration law firm Fragomen, Del Rey, Bernsen & Loewy, worked on I-9 verification for Google. The firm was breached, resulting in hundreds of employees' sensitive information leaking.
Facebook	Mexico-based media company and third-party Facebook developer Cultura Colectiva leaked more than 540M user records.
Audi + Volkswagen	An unnamed third-party vendor left a cache of more than 3.3M customers' personal data unsecured online.

CASE STUDY: TARGET AND FAZIO MECHANICAL SERVICES SECURITY BREACH	
WHAT HAPPENED?	In 2013, the payment accounts of about 41 million customers and the personal details of around 70 million were leaked from Fazio Mechanical Services (an HVAC vendor for Target), resulting in an estimated 110 million affected parties.
COST	Approximately $236 million in total expenses and more than 140 lawsuits filed against the company.
HOW DID IT HAPPEN?	Cyber attackers managed to access Target`s computer gateway by stealing credentials from Fazio Mechanical. These credentials helped the hackers exploit weaknesses in the company's systems, enter the customer service database, and install malware. Attackers accessed sensitive data such as full names, emails, credit card numbers, verification codes and more. The retailer had to pay an initial multi-state settlement of $18.5 million to cover state-specific costs associated with their investigations of the breach. Additionally, Target agreed to pay up to $10,000 to consumers who could prove their data was compromised.
WHAT WAS THE ROOT CAUSE?	Fazio Mechanical Services' data connection to the Target enterprise was compromised by a suspected Citadel Trojan. At the time of the breach, all major versions of enterprise anti-malware detected the Citadel malware. Sources claimed Fazio used the free version of Malwarebytes anti-malware – an on-demand scanning product that offers no real-time protection. Due to poor security training and lack of a comprehensive security program at the third party, the Trojan gave the attackers full range of power over Target's critical systems.
HOW IT COULD HAVE BEEN MITIGATED	Large enterprises like Target rely on the security posture of small partners like Fazio. But small partners don't have access to security software or the staff to manage it effectively. From a technology perspective, a modern security stack should have been installed onto partner computers, including next gen antivirus, endpoint detection and response, and web filtering. A mechanism should be in place, such as portal, that gives the large enterprise visibility into this protection at each partner location. Dedicated and capable security staff could have monitored for threat alerts and performed incident response activities for these small partners, stemming the worst repercussions from the breach.

References

[i] PriceWaterhouseCoopers. (n.d.). Building digital trust: Trust in third parties. PwC. Retrieved April 15, 2022.

[ii] Al Issa, A., Bailey, T., Boehm, J., & Weinstein, D. (2021, May 12). Enterprise cybersecurity: Aligning third-party cyber risk. McKinsey. Retrieved April 15, 2022.

[iii] Simmons, R. (2021, November 3). Why Managing Third-Party Access Requires A Better Approach. Forbes.com.

[iv] Miliard, M. (2020, September 24). Third-party security risk is substantial – and many providers' readiness is substandard. Healthcare IT News. Retrieved April 18, 2022.

[v] Hulme, G. V. (2021, May 5). Enterprises Misplace Trust in Partners, Suppliers. Security Boulevard. Retrieved April 18, 2022.

[vi] Ponemon Institute. (2018, November). 2018 Nth Party Study Final 3. Ponemon Institute. Retrieved April 18, 2022

[vii] Aiyer, B., Anant, V., & Di Mattia, D. (2021, March 24). Securing cybersecurity for small businesses. McKinsey. Retrieved April 18, 2022.

[viii] Klugerman, Y. (2020, July 28). Third-Party Cyber Risk: 6 Facts Every CISO Should Know. Panorays. Retrieved April 18, 2022.

[ix] Deloitte. (2020, July). Third-party failures can cost companies as much as US$1 billion per incident, per a recent Deloitte survey. Deloitte. Retrieved April 18, 2022.

[x] Roman, J., & Ross, R. (n.d.). Breach Aftermath: Target CEO Steps Down. DataBreachToday. Retrieved April 18, 2022.

[xi] Security Magazine. (2021, May 7). 51% of organizations have experienced a data breach caused by a third-party. Security Magazine. Retrieved April 18, 2022.

[xii] Aiyer, B., Anant, V., & Di Mattia, D. (2021, March 24). Securing cybersecurity for small businesses. McKinsey. Retrieved April 18, 2022.

[xiii] Security Magazine. (2021, May 7). 51% of organizations have experienced a data breach caused by a third-party. Security Magazine. Retrieved April 18, 2022.

[xiv] Segal, Edward. (2022, March 16). Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report. Forbes. Retrieved April 18, 2022.

[xv] Yahoo. (2021, September 22). Organizations Deprioritize Third-Party Relationships as Potential. Yahoo. Retrieved April 18, 2022.

[xvi] Loo, E., & Gelinne, J. (2020, May 6). Adapting Your Cybersecurity Organization for the Future. Deloitte. Retrieved April 18, 2022.

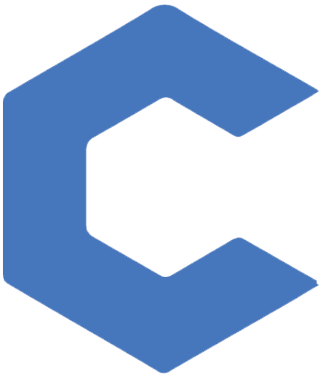
[xvii] Johnson, M. (2022, January 29). 5 Reasons Why Email Is the Top Attack Vector. Latest Hacking News. Retrieved April 18, 2022.

[xviii] Deloitte. (n.d.). Phishing and Ransomware - How can you prevent these evolving threats? Deloitte. Retrieved April 18, 2022.

[xix] Kassner, M. (2016, April 29). Cyber threat hunting: How this vulnerability detection strategy gives analysts an edge. TechRepublic. Retrieved April 18, 2022.

[xx] Loo, E., & Gelinne, J. (2020, May 6). Adapting Your Cybersecurity Organization for the Future. Deloitte. Retrieved April 18, 2022.

[xxi] PwC. ((2021, February 17). Balancing Complexity and Simplicity in Cybersecurity. PwC. Retrieved April 18, 2022.



Cylitic Security

Contact

Cylitic Security
2100 Geng Rd, Palo Alto, CA 94303

www.cylitic.com

1-888-212-6523