A New Guide to Evaluating Managed Security Services Providers

UnitedLex
Delivering Business Impact.

In 2015, more than 1.1 billion records were exposed in data breaches, according to Goldman Sachs. And the Ponemon Institute says that both the cost and volume of data breaches are rising, estimating that the average total cost of a data breach worldwide was more than $3.79 million per incident[1], and this calculation intentionally omitted the costs of "mega breaches", such as the much publicized cyberattacks on Anthem, TurboTax and the U.S. Government's Office of Personnel Management.

This comes at a time when more and more companies are dramatically increasing their spending on managed security services providers (MSSPs). So what's going on?

Traditional MSSPs boast all the latest technology, yet they struggle to detect unknown threats and aren't effectively reducing response and recovery times. Their clients still lack focus in their spending and security efforts, and their clients' legal and C-suite teams still struggle to manage the legal and regulatory aftermath of a breach.

Effective cybersecurity requires more than tools. It requires human intelligence and human analysis. The following is a guide to evaluating prospective managed security services providers and the new expectations organizations should have if they truly expect an MSSP to reduce risk, cost and tactical burden.

Limitations of the Traditional MSSP Model

There is no fool-proof security measure, nor is there a magic bullet to catch and stop every attacker, but it is clear that the traditional IT-centric, tools-based cybersecurity methods are inadequate. The gap between breach and detection is growing[2] and most companies still struggle to contain and remediate threats in time to prevent widespread damage, which is why data breach costs are increasing year over year.

More and more organizations are turning to service providers thinking they will reduce detection and response times, improve cyber risk mitigation, and reduce costs throughout the cybersecurity lifecycle. However, the traditional MSSP model is also IT-centric and tools-based. When traditional methods are clearly falling short, why would doubling down on more of the same solve the problem?

Any client hoping to maximize return on investment in an MSSP should ensure that the provider can overcome the obstacles that lie at the root of the problem:

- Prioritizing risk and security efforts.
- Expanding threat detection to include unknown threats and data leakage.
- Enabling proactive threat detection.
- Offloading the tactical burden of threat validation and incident response.
- Mitigating not just operational costs, but the business and legal costs of a breach, as well.

Knowing where your risk lives, prioritizing security efforts and identifying anomalies indicative of unknown threats, such as advanced targeted attacks and compromised credentials are all still very much human activities. They require human intelligence and human analysis. Cybersecurity programs must involve all of a company's stakeholders—company executives, the board of directors, the IT department, legal and compliance teams, and more—throughout the entire cybersecurity lifecycle.

1 Ponemon Institute (2015) Cost of Data Breach Study: Global Analysis
2 Verizon (2015) Data Breach Investigations Report

Skillset, Technology and Stakeholder Collaboration Deficits

Findings from the Ponemon Institute's 2014 study on data breach preparedness[3] illustrate Information Security departments' skillset, technology and stakeholder collaboration deficits. According to the study, less than 1/3 have advanced threat detection technologies and only 20% are able to conduct continuous monitoring, while more than half lack the skilled practitioners to deploy and manage these advanced capabilities. If an organization fails to achieve effective automation and precision monitoring for known threats, it will never have the bandwidth to proactively hunt for unknown threats.

Seventy percent of data breach preparedness respondents reported that they need more senior-executive involvement in planning, and 78 percent said they fail to review their incident response plans – even just annually. In addition, only 42 percent of companies surveyed in the Global State of Information Security report say their Board actively participates in the overall security strategy and just 36 percent say the Board is involved in security policies.[4] These statistics clearly explain the ever-increasing costs of data breaches. Failure to test one's incident preparedness practically ensures labored and ineffectual response processes, and without stakeholder involvement throughout the "prevent – detect – respond" lifecycle, the broader organization is ill-equipped to address the business and legal fallout of a breach.

Relying on IT-centric providers that operate with only a cursory understanding of a client's business environment, data universe and end user behaviors makes it difficult to develop a comprehensive security program that truly overcomes skillset, technology and stakeholder collaboration deficits. The ever-increasing volume and sophistication of cyber attacks demands that MSSPs develop a model that supports more than compliance logging or automated known threat monitoring. They must learn to deliver unknown threat detection and proactive threat hunting, effectively alleviate tactical burden during incident response, and also address the needs of legal, compliance and executive teams.

Stakeholder Intelligence: The Foundation of Effective Cybersecurity

There are plenty of security service providers offering "advanced threat detection" and "intelligence-driven" security, but the intelligence they are referring to is threat intelligence that, in practice, is only suited for detecting known threats, and it's not enough. What's needed, and what should be the foundation of any cybersecurity program, is stakeholder intelligence. Having a comprehensive understanding of your company operations, your employees, your data, and your customers will be the decisive factor

QUESTIONS
To Ask Prospective MSSPs

1. How will you gain an understanding of my operations, end user behaviors and business requirements?
2. Do you have expertise in the specific regulatory and compliance requirements of my business?
3. How do you develop a threat profile?
4. How do you coordinate security and compliance activities between Information Security and Legal?
5. How do you coordinate security and compliance activities between IT and legal teams?
6. How do you monitor for and identify *known* threats?
7. How do you monitor for and identify *unknown* threats?
8. Do you offer any legal services, such as e-discovery and legal staffing, to facilitate a seamless transition from incident response to litigation?

Failure to test one's incident preparedness practically ensures labored and ineffectual response processes.

3 Second Annual Study on Data Breach Preparedness, September 15, 2014, Ponemon Institute
4 PWC (2015) Global State of Information Security Survey

in mitigating cyber risk, expanding threat detection, and optimizing incident response and its associated legal and regulatory matter management. Integrating this intelligence from the get-go enables more effective regulatory planning and enforcement; effective prioritization of risk, efforts and investments; more precise monitoring; better identification of anomalies; and a holistic incident response plan that addresses the needs of all company stakeholders.

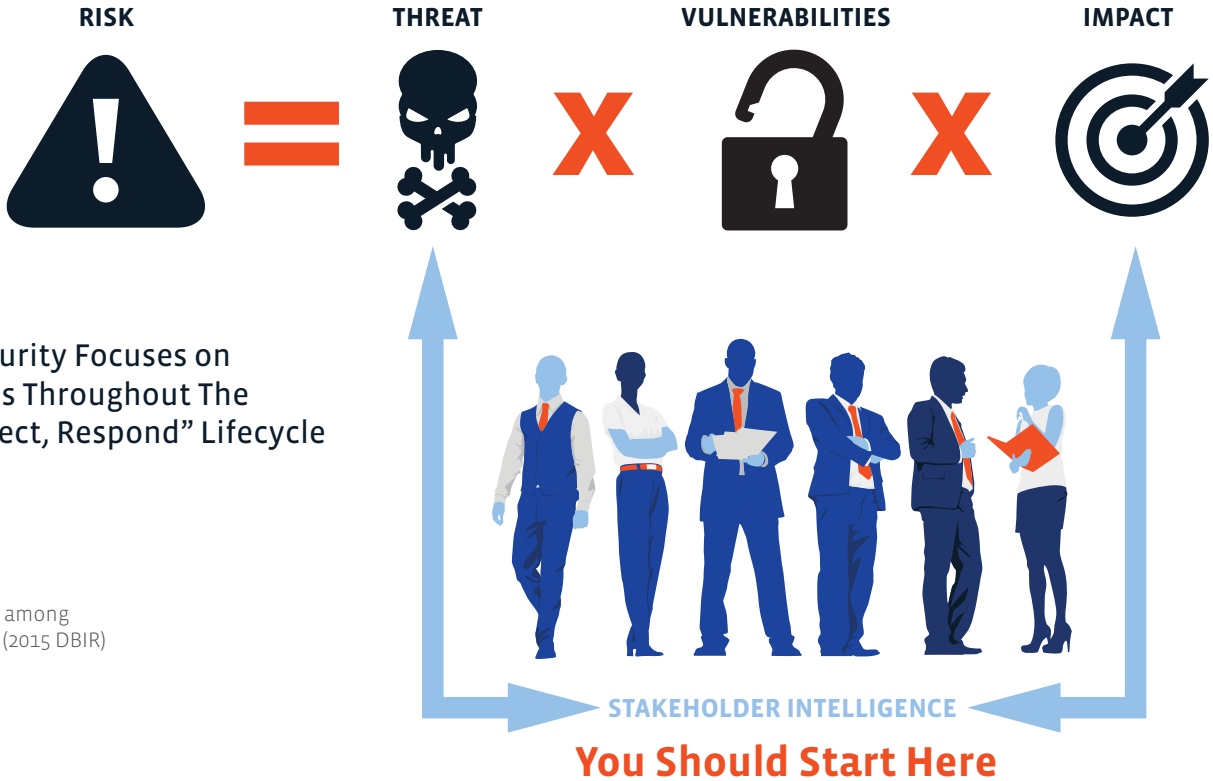
In addition, human intelligence and human analysis ensures security efforts are tailored to a company's unique threat profile. For example, an investment firm's threat profile likely differs from that of a United States "big 4" bank. For that investment firm, devoting budget and resources to address a generic "financial services" threat profile would not only dilute efforts, but would likely be a waste of money. Capitalizing on your company's human intelligence and combining it with a security provider that leverages that intelligence and augments it with guidance and support for your legal and compliance teams will help you remain laser focused on the cyber risk most relevant to your business.

A Multi-disciplinary, Converged Approach Driven by Stakeholder Intelligence

The following section should serve as a guide in evaluating managed security services providers, as it maps key elements of a more forward-leaning, converged approach to each stage of the cybersecurity lifecycle.

RISK ASSESSMENT AND STRATEGY DEVELOPMENT

Traditionally, when an organization engages an MSSP to deliver a risk assessment, the first thing that MSSP does is take an inventory of assets and run a vulnerability scan. However, the first thing an MSSP should do is bring all stakeholders to the table to map the regulatory and legal risk at the IT, human and third-party layers. Make sure your provider is ranking risk by potential legal and business impact and calculating the likelihood of threats associated with that risk. Then the provider can identify security gaps, assess incident readiness and help you develop targeted security and response processes based on those calculations of likelihood and impact potential.

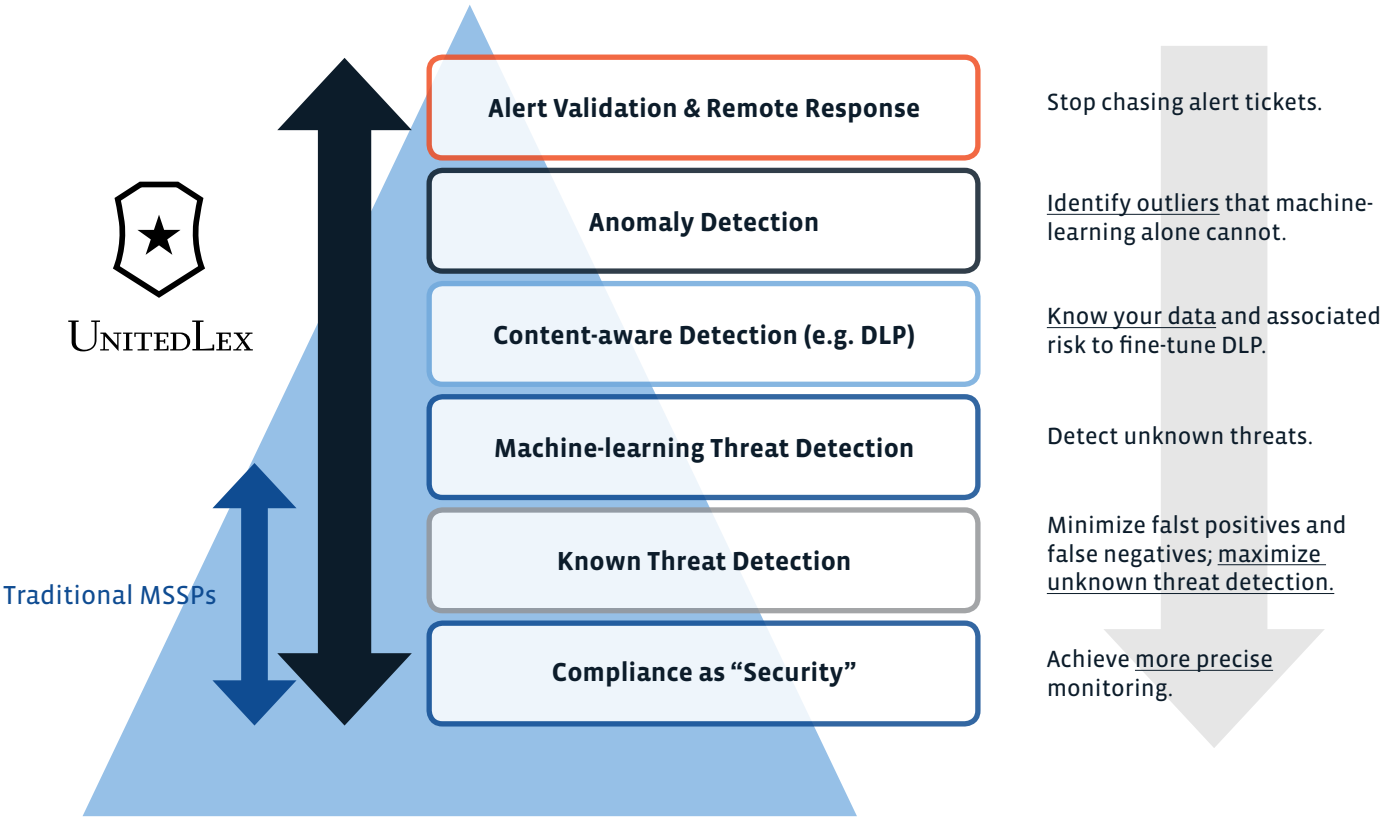


IT-Centric Security Focuses on Vulnerabilities Throughout The "Prevent, Detect, Respond" Lifecycle

Threat profiles differ among industry subscribers (2015 DBIR)

MANAGED SECURITY SERVICES

Managed Security Services should complement your existing capabilities with more precise monitoring, expanded detection, and seamless threat validation and response that provide insights derived from a unique set of post-exploitation analytics. The MSSP should be facilitating ongoing multi-stakeholder collaboration to deliver value beyond information security, increasing your organization's ability to reduce the operational, legal and business impacts of a breach.



An MSSP with legal and compliance expertise can gather non-technical stakeholder intelligence to paint a comprehensive picture of your business operations, data universe and user behaviors, then apply that intelligence to enable context- and content-aware monitoring, as well as proactive threat hunting via sophisticated correlation and user behavior analytics.

While indicators of compromise and other threat identifiers should be leveraged, this should not be the only detection method. A decisive factor in expanding threat detection is the continual, active analysis of skilled security practitioners. It is possible for an MSSP to work collaboratively, as an extension of your security team to implement this added layer of human analysis in an affordable and scalable way, and this level of support should be discussed when vetting MSSPs. There is a marked increase in value for the client as compared to the IT-centric model employed by traditional providers.

INCIDENT RESPONSE AND REMEDIATION

Organizations should consider a managed incident response service, in which the MSSP has remote visibility and reach into the client's network to enable immediate remote response at the onset of an incident. Often, under the traditional model, the MSSP relies on the client's already resource-constrained team to validate alerts and contain threats, and the service provider's response team frequently arrives on site with little or no knowledge of the client's infrastructure or investigative findings up to the point of the MSSP's arrival. The delays associated with these limitations can result in far greater impact to an organization. Further any MSSP engaged to assist with incident response should be capable of conducting its investigation with legal and regulatory matter management in mind, ensuring that ample evidence is preserved to support investigatory conclusions, providing actionable deliverables

for the legal and C-Suite teams throughout the process, and determining the scope and scale of a compromise as quickly and as accurately as possible so the client can make informed legal and business decisions.

Speed, accuracy and alignment of the internal and external response teams at the onset of a breach are vital components to reducing cost and impact.

ACHIEVING AN ADAPTIVE SECURITY PROGRAM WITH ONGOING STRATEGIC SUPPORT

When evaluating an MSSP, ask how it can help you achieve an adaptive security program. How does the MSSP deliver continual support to ensure all strategic and tactical gaps are filled? How does it facilitate continuous refinement driven by stakeholder intelligence and lessons learned during the course of fire drills, incident response or proactive security assessments?

Conclusion

When an MSSP is enlisted to optimize a cybersecurity program for any organization, it must begin with human intelligence and human analysis. UnitedLex involves stakeholders from across the organization, taking the time to understand the client's business operations, data universe and user behaviors to tailor a security program to an organization's business and legal needs. This multi-disciplinary, converged approach is the answer to overcoming the limitations that prevent IT-centric MSSPs from solving a client's most critical challenges:

- Prioritizing risk and security efforts.
- Expanding threat detection to include unknown threats and data leakage.
- Enabling proactive threat detection.
- Offloading the tactical burden of threat validation and incident response.
- Mitigating not just operational costs, but the business and legal costs of a breach, as well.

The advantages of bridging gaps between Information Security and non-technical stakeholders extends beyond benefits, such as better prioritization of budget and efforts, and achieving a seamless transition between incident response and legal and regulatory matter management. By involving legal and business stakeholders in defining the company's risk landscape and in applying institutional intelligence to improve prevention and detection, Information Security leaders are actually facilitating executive buy-in on their security strategies and investments.

An MSSP that can establish stakeholder alignment and leverage stakeholder intelligence is best suited to be a strategic partner in ensuring the client has a defensible, actionable and adaptive security program that realizes the full value of security investments while reducing the cost and impact of a breach.

About UnitedLex

As a global provider of technology powered legal and business services, UnitedLex delivers industry leading legal and cyber risk strategies and solutions. UnitedLex was founded in 2006 with a singular mission to improve the performance of leading corporations and law firms and academic institutions. Since then, UnitedLex's more than 1,800 attorneys, engineers and consultants have provided unparalleled solutions resulting in risk mitigation, efficiency improvements and cost optimization for its clients around across the globe. With more than $250 million in assets and committed capital, UnitedLex deploys the right blend of service and technology to support the world's leading corporations and law firms.

Contact us at information@unitedlex.com