Cybersecurity As A Service

Pillsbury Global Sourcing

June 3, 2014

Presentation Summary

- Part 1: Current State of Cybersecurity
  - Policy Landscape
  - Trends within Organizations
- Part 2: Managed Security Services (MSS) Description
  - Summary of the Service
  - The Benefits of Managed Security Services
  - Trials and Tribulations of Procuring MSS
- Part 3: Using Managed Security Services as part of a Comprehensive Cybersecurity Program
- Part 4: Five Things To Know About Cybersecurity

pillsbury

Current State of Cybersecurity

pillsbury

What is Cybersecurity?

- "Cybersecurity is technology, processes and practices employed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access."

  - SEC Cybersecurity Disclosure Guidance

- "Cybersecurity is not all about technology, it's much bigger than that; it's a business challenge…the impact on their bottom line isn't virtual; it's real, so companies [had] better start thinking about it as a real, honest-to-goodness business problem."

  - Former Secretary of Homeland Security Tom Ridge in September 2013

- Cyber attacks include:
  - hacking to steal data or assets or to corrupt data
  - causing operational disruptions
  - causing a website to fail (DNS attacks)

pillsbury

The Threat: Ripped from the Headlines

Experts Warn of Coming Wave of Serious Cybercrime

The rash of attacks against Target and other top retailers is likely to be the leading edge of a wave of serious cybercrime, as hackers become increasingly skilled… - The Washington Post, February 2014

51% of CEOs surveyed say their company experiences cyber attacks hourly or daily - Ponemon Institute

- **Trends**
  - It takes an average of 243 days before an attack is detected
  - Attackers increasingly exploit weaknesses in third party suppliers' networks to access the target company
  - A significant number of attacks are originating from China
  - Attacks are concentrated on key industries – energy, financial services, and retail
  - Once a company is targeted, attackers will return

pillsbury

Overview of Cybersecurity Legal Authorities

Who is Responsible?

- Federal
  - Department of Homeland Security
  - Department of Energy
  - Department of Treasury
  - Department of Commerce
    - NIST, NSF, FTC
  - Department of Justice
  - Department of Defense
  - Securities Exchange Commission
  - Nuclear Regulatory Commission
- States
  - State Attorney Generals
  - Offices of Consumer Affairs and Business Regulation
- International Governments
  - European Union
- Trade Associations / Industry Groups

As a result, an ever complex array of domestic and global regulations is being enacted to protect the public from cyber attacks

pillsbury

U.S. Cybersecurity Policy (Feb. 12, 2013)

- Executive Order 13636 - Improving Critical Infrastructure Cybersecurity
  - Develop a technology neutral Cybersecurity Framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Explore the use of existing regulation to promote cybersecurity
- Presidential Policy Directive 21 (PDD-21) - Critical Infrastructure Security and Resilience
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan

NIST Cybersecurity Framework

- Framework for Improving Critical Infrastructure Cybersecurity v1.0 and a Roadmap for future cyber efforts were officially released on Feb. 12, 2014
- A risk management framework for assessing the risk of cyberattack, protecting against attack and detecting intrusions as they occur.
  - Comprised of 5 Key Functions – Identify, Protect, Prevent, Respond, Recover
  - Maturity "Tiers" – Partial, Risk-Informed, Repeatable, Adaptive
- Includes guidance for how to respond and recover from an attack
- Most significant change in the final version related to privacy-protection portions of the Framework
- BUT… it is has been criticized for being too vague and toothless
  - Security experts say the framework is not that different from the checklists chief security officers regularly implement

pillsbury

International Initiatives – The European Union

- Cyber Security Strategy of the European Union
  - Aims to combat cybercrime by introducing minimum requirements for Network and Information Security (NIS) standards across Europe
  - Potential global impact
- Proposed EU Directive on Network and Information Security
  - Would establish Computer Emergency Response Teams in each Member State
  - Oblige Member States to adopt their own NIS strategy
  - Promote information sharing between private sector and authorities
    - Member States to ensure that public administration and market operators notify all incidents
    - Mandated reporting on incidents with a potential or actual impact
- Organizations that suffer a breach because they lack sufficient IT security could face fines of up to 2% of their annual global revenue (or more if the European Parliament gets its way!)

What is really happening inside Corporations?

- According to a recent Ponemon Institute survey, CIOs and CISOs often skirt the naked truth about cybersecurity within their organization … 55% of those IT security workers polled said they make assertions that they can't actually support, including offering assurances that "it's been taken care of"

- Why the obfuscation?

- To-date many companies:
  - Have made significant investments in cybersecurity tools
  - Handle cybersecurity in a piecemeal fashion
  - Tend to be more focused on response to incidents rather than prevention

Helping Corporations Mature Capabilities

- New Operating Models are needed for companies to mature corporate cybersecurity capabilities
  - Defensive advantages must be created from improved processes and organization
- Corporations need to more holistically manage their enterprise-wide cybersecurity programs
  - The focus should be on strategic decision-making and management vs. day-to-day operational tasks
- Who should this resonate with?
  - CEOs and Boards can no longer hide from this issue!
  - Are we moving toward increased executive level accountability for cybersecurity (i.e., Sarbanes Oxley)?

Managed Security Services Description

pillsbury

What is a Managed Security Service?

A Managed Security Service is an IT Security service outsourced to and delivered by a service provider. This service is comprised of overarching business processes that go beyond the individual configuration item (asset) focused security hygiene processes performed by IT operations or an IT Infrastructure service provider

Security Hygiene Processes

- Security Implementaion
- Security Administration
- Security Enforcement
- Credentials Management

Managed Security Processes

- Security Solution Development
- Security Operations
- Security Analysis
- Security Incident Response
- Vulnerability Assessment

Why outsource these critical security processes?

- Pillsbury has had unusual insight into IT Infrastructure operations and organizations over the last 25 years. We have observed that DIY operators:
  - Lack and lag industry best practices (e.g. ITIL, PMIBOK, CoBIT, etc.)
  - Processes are generally over-tooled and under-implemented
  - Asset management hygiene is poor
  - Lack process maturity and discipline in key overarching service management and integration processes (ITSM)
  - Rarely can afford to make the significant standalone investment in skills and resources to meet difficult process and integration challenges
  - Except in special circumstances cannot attract and retain the subject matter expertise to contain and mitigate high velocity of change risks
  - Experience lift and value creation in outsourcings using best practices coupled with rationalized tooling, mature process, automation and leveraged skills

We are seeing direct parallels between Security Management and ITSM

pillsbury

Benefits of using a Managed Security Service

- Level out the playing field vs. the black hats
  - Deployment of best practices supported by mature business processes and complimented by architected, integrated, operational and automated tooling
  - Centers of Excellance consolidating and leveraging threat intelligence and deep, competitively capable, subject matter expertise
  - Sustainabilty over the long term, both “same stuff different day” and adaptabilty to a changing threat landscape
- Benefit from lessons-learned without having to actually experience them
- Allocation of Risk
  - Reputational and other risks shared with the service provider

Cyberattacks will be very difficult to counteract without skilled allies

pillsbury

Who needs a Managed Security Service?

- It is likely that every enterprise will need some form of Managed Security Services but those who need an overarching independent service are likely to have:
  - A complex IT infrastructure — especially those with complex multi delivery actor delivery fabrics
  - An emerging collection of disparate cloud and SaaS solutions — especially those creating an internetwork of these disparate services
  - A large number of endpoints (100k+) — especially those that are physically exposed, e.g., SCADA, POS, etc.
  - Possess personal information about individuals — especially health and financial information
  - A regulatory need
  - A brand built on (and dependent on) reputation

pillsbury

Why is MSS hard to procure

- An IT services deal has several basic components:
  - MSA - the basic legal terms and conditions governing the relationship
  - Scope - describes the what that needs to be done
  - Service Levels - how well the provider will commit to perform
  - Price - the charges for the various services
  - Solution - how the supplier will provide the services

- The main buyer difficulties are:
  - Establishing an acceptable risk allocation in the legal terms
  - Describing the scope of what is to be done — the suppliers propose the how
  - Allocating the processes between actors (Client, ITO, MSS, Colo, Cloud, etc.)
  - Describing the service performance regime
  - Determining the right things to pay for — obtaining good fixed:variable ratios
  - Gathering the right information for the go-to-market cycle and minimizing due diligence effort and pricing risk

pillsbury

What is Pillsbury doing…

To make doing an MSS deal faster, cheaper, better

- Creating a standardized MSA term sheet specifically targeted at MSS deals
- Revising our Patented ValueChain Mosiac Process Reference Model to extend and enhance V1.0 of the Mangaged Security Services Process defintions
- Creating a best practice service performance regime
- Establishing pricing “buckets” in a specialized pricing model
- Developing a series of standardized data collection templates which allow MSS to be sourced in a competive environment (no supplier “studies” or invasive probes, no “kick the can down the road”, no due dilligence surprises)
- Providing suppliers with a standardized outline for solution documention

Then…

- Currently vetting our next version of the what and the fact discovery information with several major suppliers of Manged Security Services AND…
- Create competition thru terms, supplier solution, service level metrics and price

Foster vigorous competition based on how, how well and how much

pillsbury

Using Managed Security Services as Part of a Comprehensive Cybersecurity Program

pillsbury

It's About More than Just Buying the Service!

- Assess corporate cyberinsurance policies in conjunction with procuring Managed Security Services
  - Negotiate for lower premiums following a successful implementation
  - Having the appropriate policy may reduce some contracting pressures around risk allocation/limitations of liability
  - Be wary of policy terms that could eviscerate your coverage
- Robust contract management over lifecycle of Agreement
  - It will not be good enough to buy the Service and have a sound contract - companies will need to manage to it / monitor compliance to truly mature their security capabilities
- Governance and Audit
  - Managing and auditing service provider performance is crucial

Five Final Points To Consider

pillsbury

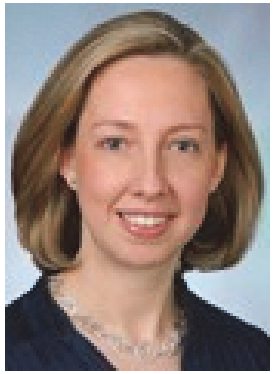
Five Parting Points on Managed Security Services

- The current regulatory / political environment is ripe for legislative action and continued government involvement
- Corporations should look to “Centers of Excellence” / Third Party Providers to mature corporate cybersecurity capabilities
- It is likely that every enterprise will need some form of Managed Security Services
- Choose an advisor that can navigate you through a comprehensive cybersecurity program inclusive of prevention, management, response and recovery
- Using Managed Security Services is more than just signing a contract – cyberinsurance, robust governance and audit models, and contract management are also crucial

pillsbury

Presented By Pillsbury Global Sourcing

Joseph Nash
Pillsbury Global Sourcing
Washington, DC
+1.202.663.8386
joseph.nash@pillsburylaw.com



Meighan O'Reardon
Pillsbury Global Sourcing
Washington, DC
+1.202.663.8377
meighan.oreardon@pillsburylaw.com

pillsbury