Building a Business-Centric IT Security Program
Presentation Overview

Critical Assets

Risk Treatment Planning

Staffing Models

Extending Programs to the Cloud
What are Critical Assets

“Data is a precious thing and will last longer than the systems themselves.”

– Tim Berners-Lee, inventor of the World Wide Web
Examples of Critical Assets

**Critical Asset** - A piece of information or data that, if compromised or leaked could cause irreparable harm to an organization.

- Product Formulas
- Product Designs
- Research Information
- PII
- Transaction Information
# Threats Against Critical Assets

## Hacktivism
Hacktivists use network exploitation to advance their political or social causes.

## Crime
An individual or group who steals information and extorts victims for financial gain.

## Espionage
Nation-states who conduct operations to steal state secrets or other proprietary information from private companies.

## Insiders
Trusted personnel and employees who steal information for personal, financial or ideological reasons.

## Terrorism
Terrorist groups that target systems that operate the country’s critical infrastructure such as water plants.

## Warfare
Nation-states sabotaging military and critical infrastructure systems to gain advantages during conflicts.

Source: Federal Bureau of Investigation Las Vegas Field Office – Cyber Division
Information Management Life Cycle

**CONTENT**

The data identified as a critical asset to be protected.

**COMMUNITY**

The people who should and should not have access to the asset.

**CHANNEL**

The allowable methods by which the asset may be transmitted.
“It takes 20 years to build a reputation and 5 minutes to ruin it and if you understand this you will do things differently”

– Warren Buffett, CEO of Berkshire Hathaway
Risk Treatment Strategies

- Risk Acceptance
- Risk Avoidance
- Risk Transferrence
- Risk Mitigation
### Quantifying Risk Mitigation

**ALE = SLE \times ARO**

<table>
<thead>
<tr>
<th>Annual Loss Expectancy</th>
<th>Single Loss Expectancy</th>
<th>Annual Rate of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Expressed in an annualized financial impact</td>
<td>Financial Impact of the loss of a single record</td>
<td>Estimated number of records that will be lost per year*</td>
</tr>
</tbody>
</table>

*Value can be less than 1
Staffing Models

“If you think hiring professionals is expensive, try hiring amateurs”

– Anonymous
Programmatic Objectives

Data Protection

Threat Protection
Staffing Needs?

Data Protection

- Security Platform Engineer
- Senior Program Analyst
- Triage Analyst
- Data Protection Analyst
- Senior Program Analyst

- Application Management
- Rule and Policy Governance
- Event Triage
- Incident Management
- Reporting and Analytics

Threat Protection

- Security Platform Engineer
- Cyber Security Intelligence Expert
- Threat Response Analyst
- Threat Response Analyst
- Security Platform Engineer

IntelliSecure
Coverage Factors

Which functions can be covered during business hours, and which need to be 24x7x365?

- It takes 5 people per skill set to cover a 24x7 schedule if each person works no more than 40 hours (Can cover with 4 if one person works 48 hours)
- In order to allow for PTO to be taken, 6 full time people per skill set are required
- Best Practices stipulate you should have 9 people per skill set in order to leave time for cross training, training, PTO, account for turnover, etc.
- Business requirements often stipulate 24x7 coverage
- The cost/benefit analysis is rarely favorable
- Managed Security Services Providers may be a good option when 24x7 coverage is needed but the cost of internal staffing outweighs the benefit.
Staffing Challenges

2016 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION:
PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014

97%
BELIEVE APTs REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY

MORE THAN
1 IN 4
ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK

$150 MILLION:
AVERAGE COST OF A DATA BREACH BY 2020

1 IN 2
BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION’S INTERNET OF THINGS (IOT) DEVICES

74%
BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM

Too Few Professionals

2 MILLION:
GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019

3X
RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14

84%
ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED

77% OF WOMEN
SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER.

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.

Image Credit: ISACA
"The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do."

-Larry Ellison, Founder and Chairman of Oracle
Growth of the Cloud

• The average employee actively uses 36 cloud services at work, including nine collaboration services, six file sharing services, and five content sharing services

• 18.1% of all documents uploaded to the cloud contain sensitive information – Skyhigh Networks

“Through 2020, 95% of cloud security failures will be the customer’s fault”

Top Predictions for IT Organizations and Users for 2016 and Beyond

Companies that embrace the cloud grow 19.6% faster

Of documents shared externally contain sensitive content
Cloud Access Security Brokers

CASB = Cloud Access Security Broker -- Security policy enforcement point between cloud service users and cloud service providers; applies enterprise security policies as cloud resources are accessed

Gartner’s 4 pillars of required CASB functionality

<table>
<thead>
<tr>
<th>Visibility</th>
<th>Compliance</th>
<th>Data Security</th>
<th>Threat Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gives orgs visibility into users, services, data, devices</td>
<td>File content monitoring to find and report on regulated data in the cloud</td>
<td>Additional layer of protection including encryption</td>
<td>Analyzes traffic patterns to ID compromised accounts and malicious usage.</td>
</tr>
</tbody>
</table>

Typical CASB Use Cases:

• Prevent sensitive data from upload to the cloud – encrypt or tokenizing data within enterprise
• Detect sensitive data already in cloud – DRM, encryption, sandbox, deletion
• Enforce differing levels of data access and cloud service functionality based on the user’s identity, device, location, and operating system
• Identify cloud apps being used by organization (Shadow IT), by whom, and risks they pose to the organization
• Evaluate and select cloud services that meet security and compliance requirements
• ID threats and potential misuse of cloud services – unusual account activity, malware
Classify Assets into Three Categories

- Public Information
- Sensitive Information
- Restricted Information
Top 5 Cloud Security Considerations

1. Define categories of information that can be shared, what can be shared with restrictions, and what cannot be shared via the cloud.
2. Ensure your Cloud Security solution allows you to comprehensively enforce the rules you have set out in Consideration 1.
3. Implement an encryption strategy that allows you to confidently share information in the cloud.
4. Implement two factor authentication to make it more difficult to access cloud resources with stolen credentials.
5. Monitor user behavior with respect to cloud usage for signs of Insider Threat or misuse.
Key Takeaways

1. Identify Business Critical Information Assets and understand their life cycle

2. Model Your Risk Against those assets to identify and apply appropriate protections universally wherever those assets exist

3. Define staffing needs and develop a strategy to meet those needs
QUESTIONS?

Connect with Us!

InteliSecure
@InteliSecure

Jeremy Wittkop
@JeremyWittkop
Building a Comprehensive IT Security Program

Practical Guidelines and Best Practices

Jeremy Wittkop