Building a Next Generation Security Architecture

Michael J. Lewis
Senior Staff Security Strategist
Chevron
Michael.J.Lewis@chevron.com
Introduction to the presentation: Building a security architecture

- Justify Building / Revising the Security Architecture
- Set Guiding Principles
- Identify and Evaluate Risks
- Select Controls
- Publish and Implement Architecture
Technique #2

Shout [someone else’s] “Data Breach” at the top of your lungs.
Technique #3: Develop a Business Case

- Oil and Natural Gas (ONG) Business Models
- Regulation
- Technology
- Threats
Information security challenges with Oil and Natural Gas business models

- Joint ventures and partnerships
- Specialized computing environments
  - Process Control
  - Supervisory Control And Data Acquisition (SCADA)
- Exotic environments
Cyber security regulation applicable to Oil and Natural Gas Industry

- Sarbanes-Oxley (2002)
- State data breach notification laws (first in 2002)
- Chemical Facility Anti-Terrorism Standards (CFATS) (2007)

- Department of Energy (DOE) ONG Cybersecurity Capability Maturity Model (C2M2) (2012)
- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (2014)
- Cybersecurity Information Sharing Act (2015)
- Etc. Etc. Etc. Etc…………………
Cyber security regulation applicable to Oil and Natural Gas Industry

- Privacy
- Localization
- ISO 27000 (2005 and 2013)
- In progress European Union work
  - Network and Information Security Directive
  - Data Protection regulation
Technology Shifts (2005)

- A cloud was a meteorological event
Technology Shifts (2005)

- The only thing that “tweeted” were birds
Technology Shifts (2005)

- Tablets were made of paper
Technology Shifts

- Cloud Computing
- Social Media
- Mobility
- Internet of Things
A botnet (Conficker) infected millions of new PCs for 3 years after it was 'suppressed'. - According to Computerworld's Gregg Keizer, (April 26, 2012)

The New York Times and The Washington Post have been victims of cyber-intrusions. - According to Washington Post's Craig Timberg and Ellen Nakashima (February 20, 2013)

Millions of Target customers were impacted by the Target data breach. - According to Washington Post's Jia Lynn Yang and Amrita Jayakumar (January 10, 2014)
Applying threats to Oil and Gas Industry

  - “The pace of foreign economic collection and industrial espionage activities against major US corporations and US Government agencies is accelerating.”
  - Energy and natural resources companies are among those likely to be “priority targets”
- Documented attacks / threats
  - Targeted attacks (Advanced Persistent Threats)
  - Hacktivist (like Anonymous) activities
- “Game changers”
  - Shamoon
  - Stuxnet
- Threat actors (external and internal)
Justify Building / Revising the Security Architecture

Set Guiding Principles

Identify and Evaluate Risks

Publish and Implement Architecture

Select Controls
Security is an enabler that allows the business to accomplish its mission.

Courtesy Ronald Reagan Library
Security is architected so that it is the natural path for a person to take
Re-architected Security Controls

Preventive Threat 1

Preventive Threat 2

Preventive Threat 3

Detective
Security must evolve to address future technologies and emerging threats

“Prediction is very difficult, especially about the future.”

— attributed to Niels Bohr (1885 - 1962)
Scenario Planning

Network Intrusion and Response:
- Network Firewalls
- Proxy Servers
- Intrusion Prevention Systems
- Application Gateway

System placement and trust:
- Critical Trusted Zones
- And Party Zones
- Virtual Desktop (User owned device)

Authentication/Identity:
- Group Lifecycle Management
- Provisioning
- Central Repository
- Policy Environments
- Federated Services
- Public Key Infrastructure
- Identity Management
- Service authentication and validation
- Trusted level authentication

Network Segmentation:
- Intrusion Prevention Systems
- Virtual Private Networks

Authorization:
- Common web service security
- Application security framework
- Access Management

Encryption:
- Encryption

Monitoring:
- Monitoring and Scanning Tools
- Intrusion Prevention Systems
- Threat Management / Anti-Virus
- Data Loss Management

Bring Your Own Devices

Network Intrusion and Response:
- No applicable

System placement and trust:
- Service authorization and validation
- Browser-based Thin Client

Authentication/Identity:
- Identity as a Service

Authorization:
- Software-as-a-Service

Encryption:
- Encryption

Monitoring:
- Cloud Audit
- Threat Management / Anti-virus
- Device Management

Public Cloud-based Data Centers

Network Intrusion and Response:
- No applicable

System placement and trust:
- Device authentication and validation
- Browser-based Thin Client

Authentication/Identity:
- Identity as a Service

Authorization:
- Software-as-a-Service

Encryption:
- Encryption

Monitoring:
- Cloud Audit
- Threat Management / Anti-virus
- Device Management

Restricted Client Devices

Network Intrusion and Response:
- No applicable

System placement and trust:
- Device authentication and validation
- Browser-based Thin Client

Authentication/Identity:
- Identity as a Service

Authorization:
- Software-as-a-Service

Encryption:
- Encryption

Monitoring:
- Cloud Audit
- Threat Management / Anti-virus
- Device Management
Justify Building / Revising the Security Architecture

Set Guiding Principles

Identify and Evolve Risks

Select Controls

Publish and Implement Architecture
These are risks?
Scenario modeling

- Threat modeling

<table>
<thead>
<tr>
<th>Attack</th>
<th>Motivation</th>
<th>Vulnerability</th>
<th>Threat</th>
<th>Exploit</th>
<th>Exploit</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack personal data</td>
<td>Cross-site scripting</td>
<td>Improper exception handling</td>
<td>Deny</td>
<td>Relative</td>
<td>Damage</td>
<td>Physical theft</td>
</tr>
<tr>
<td>Attack sensitive data</td>
<td>Cross-site scripting</td>
<td>Improper exception handling</td>
<td>Deny</td>
<td>Relative</td>
<td>Damage</td>
<td>Physical theft</td>
</tr>
<tr>
<td>Attack unauthorized access</td>
<td>Cross-site scripting</td>
<td>Improper exception handling</td>
<td>Deny</td>
<td>Relative</td>
<td>Damage</td>
<td>Physical theft</td>
</tr>
<tr>
<td>Attack privileged access</td>
<td>Cross-site scripting</td>
<td>Improper exception handling</td>
<td>Deny</td>
<td>Relative</td>
<td>Damage</td>
<td>Physical theft</td>
</tr>
</tbody>
</table>

- Attack graphs

Diagram showing various threats and impacts, such as data integrity compromise, brand damage, data exposure, liability, and privacy. Various techniques such as SmartFilter, Software Composition Analysis, and DLP (Data Loss Prevention) are mentioned to mitigate these risks.
## Threat modeling

<table>
<thead>
<tr>
<th>Attacker</th>
<th>Tradecraft</th>
<th>Vulnerability</th>
<th>Action</th>
<th>Target</th>
<th>Result</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation State - high motive; high capability</td>
<td>Advertise wrong BGP routes</td>
<td>Excessive/improper access</td>
<td>Spoof</td>
<td>Ports</td>
<td>Theft</td>
<td>Financial Gain</td>
</tr>
<tr>
<td>Nation State - high motive; low capability</td>
<td>Cable physically severed</td>
<td>User behavior</td>
<td>ReRoute</td>
<td>People</td>
<td>Data loss</td>
<td>Intellectual property</td>
</tr>
<tr>
<td>Nation State - low motive; low capability</td>
<td>DNS cache poisoning</td>
<td>Zero day</td>
<td>Copy</td>
<td>IP addresses</td>
<td>Control</td>
<td>Strategic advantage</td>
</tr>
<tr>
<td>Hacktivist - Anonymous</td>
<td>SYN floods (denial of service)</td>
<td>Privilege escalation</td>
<td>Read</td>
<td>Big data</td>
<td>Destroy</td>
<td>Mayhem</td>
</tr>
<tr>
<td>Hacktivist - Lawsuit</td>
<td>Data subpoenaed</td>
<td>User manipulation</td>
<td>Probe</td>
<td>Classified information</td>
<td>Reputational damage</td>
<td>Bragging rights</td>
</tr>
<tr>
<td>Traditional attention seeking hacker</td>
<td>Targeted phishing</td>
<td>Unpatched systems</td>
<td>Bypass</td>
<td>Customer data</td>
<td>Monetary loss</td>
<td>Damage economy</td>
</tr>
<tr>
<td>Opportunist</td>
<td>SQL Injection</td>
<td>Posting personal data</td>
<td>Flood</td>
<td>Contacts</td>
<td>Deny</td>
<td>Industrial espionage</td>
</tr>
<tr>
<td>Malicious insider</td>
<td>Cross-site scripting</td>
<td>Insecure application development</td>
<td>Deny</td>
<td>Keys</td>
<td>Shareholder action</td>
<td></td>
</tr>
<tr>
<td>Non-malicious insider (accident)</td>
<td>Password cracking</td>
<td>Known worm/virus</td>
<td>Identity Fraud</td>
<td>Credentials</td>
<td>Regulatory investigation</td>
<td></td>
</tr>
<tr>
<td>Malicious privileged user (administrator)</td>
<td>Malware</td>
<td>Masquerade</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical theft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical attack (guns/ bullets)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Social engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Threat modeling – Example One

<table>
<thead>
<tr>
<th>Attacker</th>
<th>Tradecraft</th>
<th>Vulnerability</th>
<th>Action</th>
<th>Target</th>
<th>Result</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation State - high motive; high capability</td>
<td>Advertise wrong BGP routes</td>
<td>Excessive/improper access</td>
<td>Spoof</td>
<td>Ports</td>
<td>Theft</td>
<td>Financial Gain</td>
</tr>
<tr>
<td>Nation State - high motive; low capability</td>
<td>Cable physically severed</td>
<td>User behavior</td>
<td>ReRoute</td>
<td>People</td>
<td>Data loss</td>
<td>Intellectual property</td>
</tr>
<tr>
<td>Nation State - low motive; low capability</td>
<td>DNS cache poisoning</td>
<td>Zero day</td>
<td>Copy</td>
<td>IP addresses</td>
<td>Control</td>
<td>Strategic advantage</td>
</tr>
<tr>
<td>Hacktivist - Anonymous</td>
<td>SYN floods (denial of service)</td>
<td>Privilege escalation</td>
<td>Read</td>
<td>Big data</td>
<td>Destroy</td>
<td>Mayhem</td>
</tr>
<tr>
<td>Hacktivist - Lawsuit</td>
<td>Data subpoenaed</td>
<td>User manipulation</td>
<td>Probe</td>
<td>Classified information</td>
<td>Reputational damage</td>
<td>Bragging rights</td>
</tr>
<tr>
<td>Traditional attention seeking hacker</td>
<td>Targeted phishing</td>
<td>Unpatched systems</td>
<td>Bypass</td>
<td>Customer data</td>
<td>Monetary loss</td>
<td>Damage economy</td>
</tr>
<tr>
<td>Opportunist</td>
<td>SQL Injection</td>
<td>Posting personal data</td>
<td>Flood</td>
<td>Contacts</td>
<td>Deny</td>
<td>Industrial espionage</td>
</tr>
<tr>
<td>Malicious insider</td>
<td>Cross-site scripting</td>
<td>Insecure application development</td>
<td>Deny</td>
<td>Keys</td>
<td>Shareholder action</td>
<td></td>
</tr>
<tr>
<td>Non-malicious insider (accident)</td>
<td>Password cracking</td>
<td>Known worm/virus</td>
<td>Identity Fraud</td>
<td>Credentials</td>
<td>Regulatory investigation</td>
<td></td>
</tr>
<tr>
<td>Malicious privileged user (administrator)</td>
<td>Malware</td>
<td>Masquerade</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical theft</td>
<td>Gain trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical attack (guns/ bullets)</td>
<td>Infiltrate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Threat modeling – Example Two

<table>
<thead>
<tr>
<th>Attacker</th>
<th>Tradecraft</th>
<th>Vulnerability</th>
<th>Action</th>
<th>Target</th>
<th>Result</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation State - high motive; high capability</td>
<td>Advertise wrong BGP routes</td>
<td>Excessive/improper access</td>
<td>Spoof</td>
<td>Ports</td>
<td>Theft</td>
<td>Financial Gain</td>
</tr>
<tr>
<td>Nation State - high motive; low capability</td>
<td>Cable physically severed</td>
<td>User behavior</td>
<td>ReRoute</td>
<td>People</td>
<td>Data loss</td>
<td>Intellectual property</td>
</tr>
<tr>
<td>Nation State - low motive; low capability</td>
<td>DNS cache poisoning</td>
<td>Zero day</td>
<td>Copy</td>
<td>IP addresses</td>
<td>Control</td>
<td>Strategic advantage</td>
</tr>
<tr>
<td>Hacktivist - Anonymous</td>
<td>SYN floods (denial of service)</td>
<td>Privilege escalation</td>
<td>Read</td>
<td>Big data</td>
<td>Destroy</td>
<td>Mayhem</td>
</tr>
<tr>
<td>Hacktivist - Lawsuit</td>
<td>Data subpoenaed</td>
<td>User manipulation</td>
<td>Probe</td>
<td>Classified</td>
<td>Reputational damage</td>
<td>Bragging rights</td>
</tr>
<tr>
<td>Traditional attention seeking hacker</td>
<td>Targeted phishing</td>
<td>Unpatched systems</td>
<td>Bypass</td>
<td>Customer data</td>
<td>Monetary loss</td>
<td>Damage economy</td>
</tr>
<tr>
<td>Opportunist</td>
<td>SQL Injection</td>
<td>Posting personal data</td>
<td>Flood</td>
<td>Contacts</td>
<td>Deny</td>
<td>Industrial espionage</td>
</tr>
<tr>
<td>Malicious insider</td>
<td>Cross-site scripting</td>
<td>Insecure application</td>
<td>Deny</td>
<td>Keys</td>
<td>Shareholder action</td>
<td></td>
</tr>
<tr>
<td>Non-malicious insider (accident)</td>
<td>Password cracking</td>
<td>Known worm/virus</td>
<td>Identity Fraud</td>
<td>Credentials</td>
<td>Regulatory investigation</td>
<td></td>
</tr>
<tr>
<td>Malicious privileged user (administrator)</td>
<td>Malware</td>
<td>Masquerade</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical theft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical attack (guns/ bullets)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Social engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Objective                                    |                                |                             |                 |                 |                |                          |

- Nation State - high motive: High capability, high motive
- Nation State - high motive: Low capability, low motive
- Nation State - low motive: Low capability, low motive
- Hacktivist - Anonymous: SYN floods (denial of service)
- Hacktivist - Lawsuit: Data subpoenaed
- Traditional attention seeking hacker: Targeted phishing
- Opportunist: SQL Injection
- Malicious insider: Cross-site scripting
- Non-malicious insider (accident): Password cracking
- Malicious privileged user (administrator): Malware
Visual representations of possible attack paths and consequences

Allow “summary” of multiple (related) attacks on a single graph

Addressing any of the vulnerabilities (boxes) addresses the attack
Addressing APT: A typical targeted attack

- Individual posts personal information which hacker gains from social networking site
- Targeted phishing attack
- Unknown (Zero Day or customized) Exploit
- Unpatched vulnerability
- Individual posts personal information which hacker gains from social networking site
- Targeted phishing attack
- Unknown (Zero Day or customized) Exploit
- Unpatched vulnerability
- Individual posts personal information which hacker gains from social networking site
- Targeted phishing attack
- Unknown (Zero Day or customized) Exploit
- Unpatched vulnerability
- Malware Infects Machine
- Scan for susceptible machines
- Command / Control Communications
- Harvest authentication credentials (key logging)
- Data Exfiltration
- Data Exposure
- Brand Damage
- Liability
- Privacy
- Export
- Compliance
- Copyright
- Infected portable media is inserted into a device
Current Control Set Versus APT

- Targeted phishing attack
- Unpatched vulnerability
- Unknown (Zero Day or customized) Exploit
- Malware Infects Machine
- Scan for susceptible machines
- Command / Control Communications
- Harvest authentication credentials (key logging)
- Data Exfiltration
- Data Exposure
- Liability
- Brand Damage

- Individual posts personal information which hacker gleans from social networking site
- Infected portable media is inserted into a device
- Known worm/virus
- AV
- IPS
- Hardened Build
- Awareness
- Patching
- Build
- Hardening
- AV
- IPS
- Brand Damage
- Data Exposure
- Liability
Quantitative Risk Assessment

FAIR Risk Calibrator

FAIR iq
Putting it all together – Addressing APT

Maintain
- Patching
- Hardened build
- IPS (Intrusion Prevention System)
- Anti-virus

Maintain and Improve
- Awareness training
- Incident response (implement crisis management)

Implement
- Virtualized browser
- Specialized Threat Detection
- SIEM (Security Information and Event Management)
RSAC Conference 2015
San Francisco | April 20-24 | Moscone Center

1. Justify Building / Revising the Security Architecture
2. Publish and Implement Architecture
3. Set Guiding Principles
4. Identify and Evaluate Risks
5. Select Controls

Flowchart:
- Justify Building / Revising the Security Architecture
  - Set Guiding Principles
  - Identify and Evaluate Risks
- Publish and Implement Architecture
  - Select Controls
Optimizing risk reduction with budget

**Maintain**
- Patching
- Hardened build
- IPS (Intrusion Prevention System)
- Anti-virus

**Maintain and Improve**
- Awareness training
- Incident response (implement crisis management)

**Implement**
- Virtualized browser
- Specialized Threat Detection
- Vulnerability Scanning
- SIEM (Security Information and Event Management)

---

- Individual posts personal information which hacker glean from social networking site
- Targeted phishing attack
- Unpatched vulnerability
- Unknown (Zero Day or customized) Exploit
- Infected portable media is inserted into a device
- Known worm/virus
- AV
- Hardened Build
- IPS
- Virtualized Browser
- Patching
- Scan for susceptible machines
- Command / Control Communications
- Harvest authentication credentials (key logging)
- SIEM
- Data Exfiltration
- Data Exposure
- Liability

---

Brand Damage

Chevron

RSAC Conference 2015

33
Where we are going...

- Run quantitative risk analysis on each control
- Identify those with most impact (most reduction in risk for less cost)
- Prioritize higher those projects to implement those controls
Apply Slide

- Immediate Actions – Determine need
- Within three months – Execute the process
  - Collect business requirements
  - Build threat scenarios to identify potential attack vectors
  - Risk Assessment
  - Identify controls and execute project plan
- Long term - Recycle
Resources

- **Threat Modeling**

- **Attack Graphs**

- **Scenario Planning**
  - Peter Schwartz; “The Art of the Long View: Paths to Strategic Insight for Yourself and Your Company”; Currency Doubleday; 1991

- **Risk Assessment**
  - The Open Group™ Risk Taxonomy Standard (O-RT): [https://www2.opengroup.org/ogsys/catalog/C13K](https://www2.opengroup.org/ogsys/catalog/C13K)
  - The Open Group™ Risk Analysis Standard (O-RA): [https://www2.opengroup.org/ogsys/catalog/C13G](https://www2.opengroup.org/ogsys/catalog/C13G)
SESSION ID: ANF-W03R

Questions?

Michael J. Lewis
Senior Staff Security Strategist
Chevron
Michael.J.Lewis@chevron.com