

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: ANF-W03R

Building a Next Generation Security Architecture

Michael J. Lewis

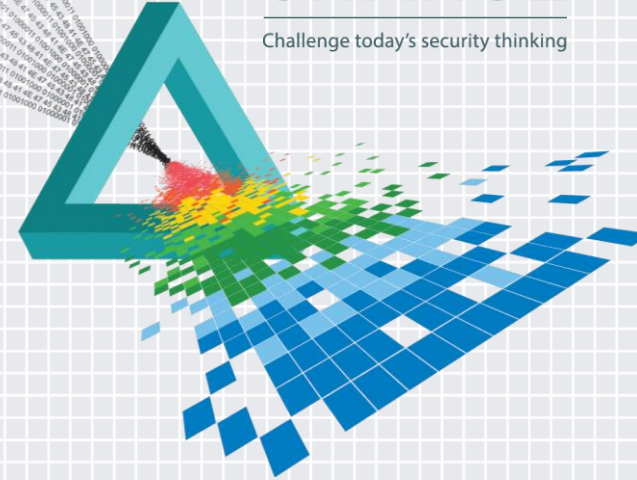
Senior Staff Security Strategist

Chevron

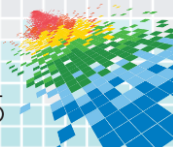
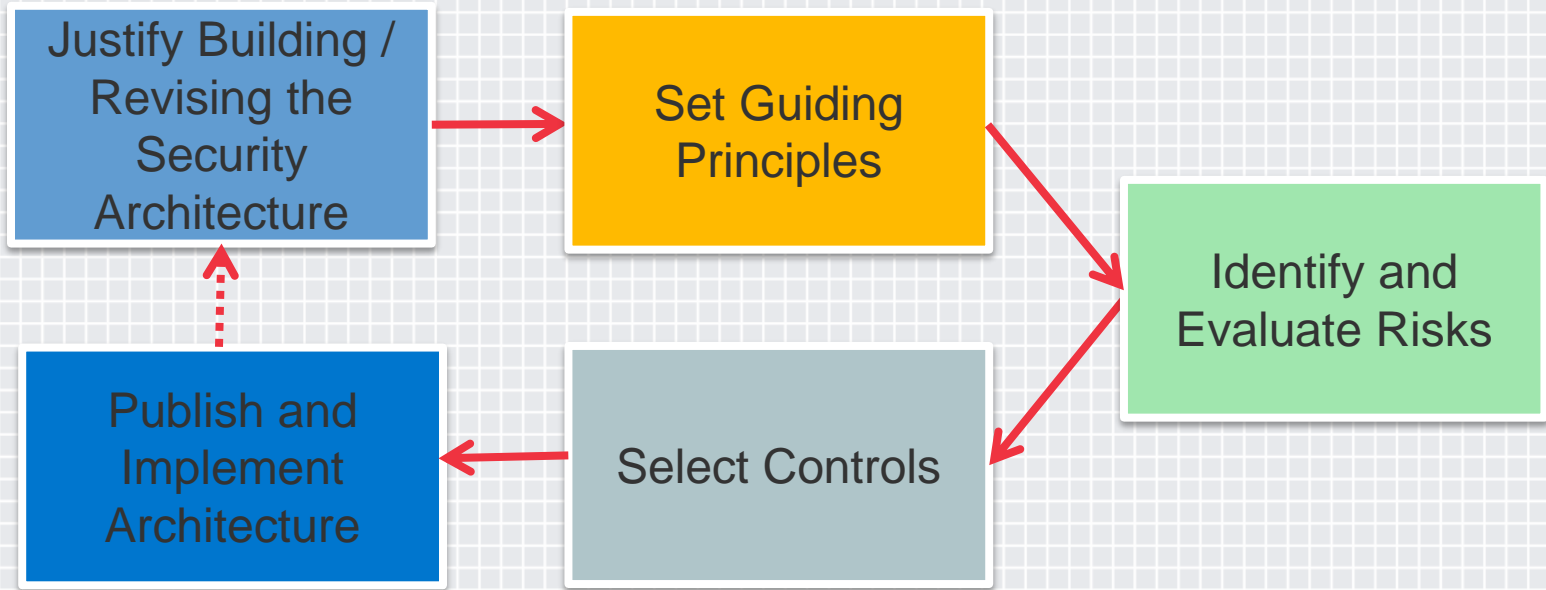
Michael.J.Lewis@chevron.com

CHANGE

Challenge today's security thinking

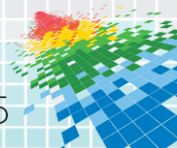


Introduction to the presentation: Building a security architecture



Technique #2

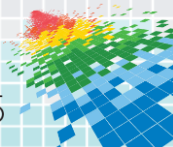
Shout [someone else's] “Data Breach” at the top of your lungs.



Technique #3: Develop a Business Case

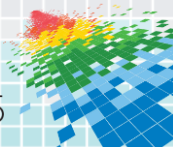


- ◆ Oil and Natural Gas (ONG) Business Models
- ◆ Regulation
- ◆ Technology
- ◆ Threats



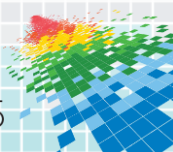
Information security challenges with Oil and Natural Gas business models

- ◆ 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 #RSAC

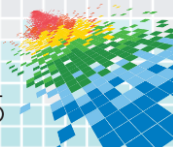
- ◆ Sarbanes-Oxley (2002)
- ◆ State data breach notification laws (first in 2002)
- ◆ Homeland Security Presidential Directive HSPD-7
- ◆ Chemical Facility Anti-Terrorism Standards (CFATS) (2007)
- ◆ Transportation Security Administration (TSA) Pipeline Security Guidelines (2008)
- ◆ Federal Energy Regulatory Commission (FERC) Critical Infrastructure Protection (CIP) (2008)
- ◆ 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)
- ◆ State of the Union proposals (Information sharing / Data Breach Notification) (2015)
- ◆ Cybersecurity Information Sharing Act (2015)
- ◆ Etc. Etc. Etc. Etc.....



Cyber security regulation applicable to Oil and Natural Gas Industry #RSAC

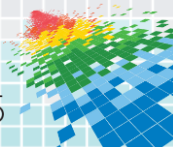


- ◆ Privacy
- ◆ Localization
- ◆ ISO 27000 (2005 and 2013)
- ◆ In progress European Union work
 - ◆ Network and Information Security Directive
 - ◆ Data Protection regulation



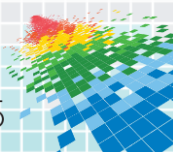
Technology Shifts (2005)

- ◆ A cloud was a meteorological event



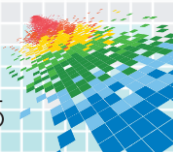
Technology Shifts (2005)

- ◆ The only thing that “tweeted” were birds



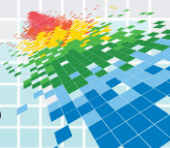
Technology Shifts (2005)

- ◆ Tablets were made of paper



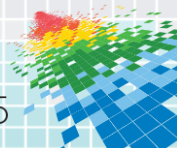
Technology Shifts

- ◆ Cloud Computing
- ◆ Social Media
- ◆ Mobility
- ◆ Internet of Things



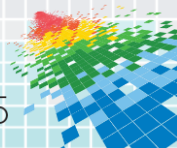
And finally, we get to threats

- ◆ 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)



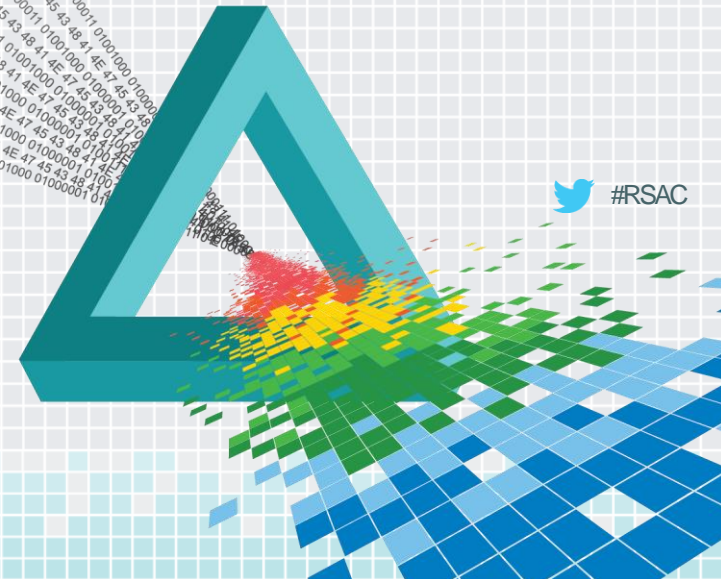
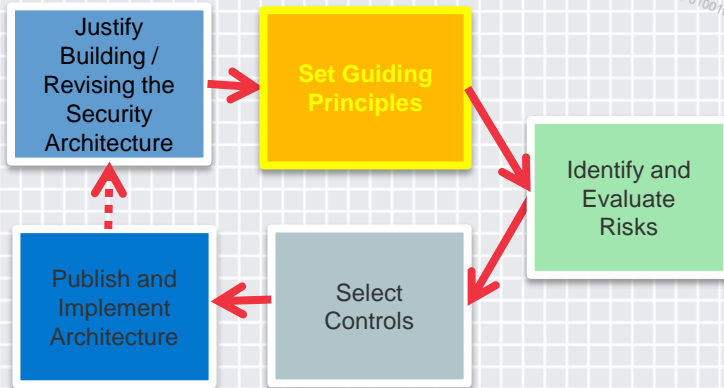
Applying threats to Oil and Gas Industry

- ◆ US National Counterintelligence Executive Report – October 2011
 - ◆ “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)
 - ◆ Hactivist (like Anonymous) activities
- ◆ “Game changers”
 - ◆ Shamoon
 - ◆ Stuxnet
- ◆ Threat actors (external and internal)



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center



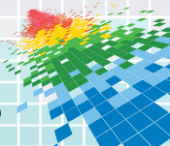
 #RSAC

Security is an enabler that allows the business to accomplish its mission. #RSAC

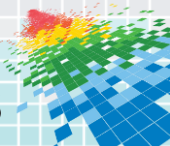


Courtesy Ronald Reagan Library

Security is architected so that it is the natural path for a person to take



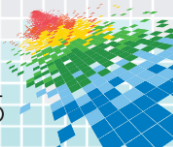
Re-architected Security Controls



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

Bring Your Own Devices

Private Data Centers

Network Intrusion and Response:

- Perimeter firewall
- Proxy servers
- Intrusion Prevention Systems
- Application Gateway

Authentication/Identity:

- Group lifecycle management
- Provisioning
- Central repository
- Policy engine
- Federated services
- Public Key Infrastructure
- Identity Management
- Device authentication and validation
- Graded level authentication

Network Segmentation:

- Intrusion Prevention Systems
- Virtual Private Networks

System placement and trust:

- Critical Trusted Zones
- 3rd Party Zones
- Virtual Desktop (User owned device)

Authorization:

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

Encryption:

- Encryption

Monitoring:

- Monitoring and Scanning Tools
- Virtual Environment
- Host Intrusion Prevention Systems
- Threatmanagement / Anti-virus
- Data Loss Management

Network Intrusion and Response:

- Perimeter firewall
- Proxy servers
- Virtual Private Networks
- Application Gateway

Authentication/Identity:

- Group lifecycle management
- Provisioning
- Directory Services
- Federated services
- Public Key Infrastructure
- RADIUS (Remote Authentication Dial In User Service)
- Policy Engine
- Device authentication and validation

Network Segmentation:

- Port Based Security
- Network Admission Control

System placement and trust:

- 3rd Party Zones
- Critical Trusted Zones

Authorization:

- Common web service security
- Application security framework (SDLC)
- Access Management

Encryption:

- Encryption

Monitoring:

- Monitoring and Scanning tools
- Threatmanagement (AV)
- Data Loss Management
- Intrusion Prevention Systems

Restricted Client Devices

Network Intrusion and Response:

- Not Applicable

Authentication/Identity:

- Identity as a Service

Network Segmentation:

- Not Applicable

System placement and trust:

- Device authentication and validation
- Browser-based Thin Client

Authorization:

- Software-as-a-Service

Encryption:

- Encryption

Monitoring:

- Cloud Audit
- Threatmanagement / Anti-virus

Public Cloud-based Data Centers

Network Intrusion and Response:

- Proxy Servers
- Virtual Branch Network

Authentication/Identity:

- Identity as a Service

Network Segmentation:

- Not Applicable

System placement and trust:

- Device authentication and validation
- Browser-based Thin Client

Authorization:

- Software-as-a-Service

Encryption:

- Encryption

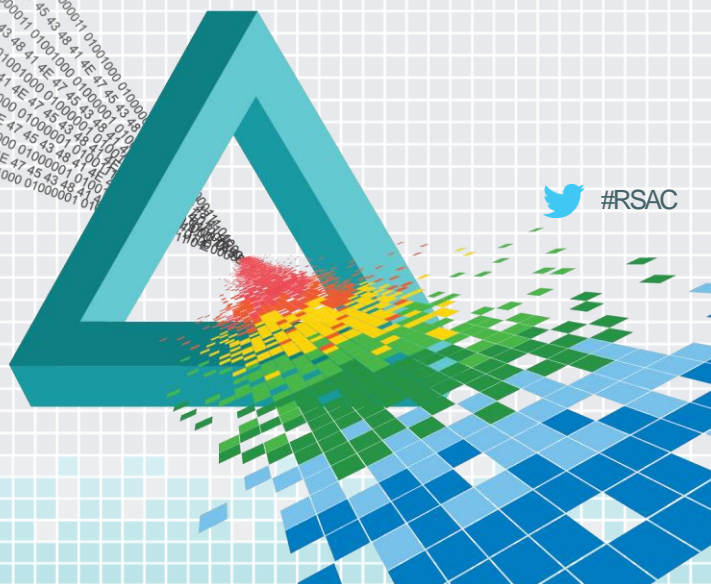
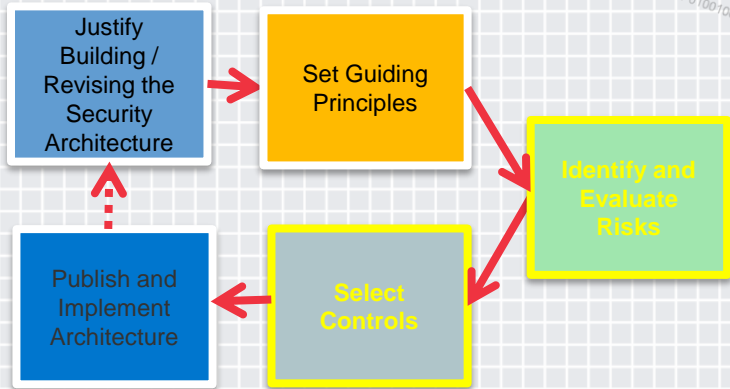
Monitoring:

- Cloud Audit
- Threatmanagement / Anti-virus
- Device Management

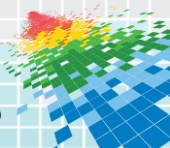


RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center



These are risks?

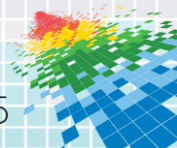
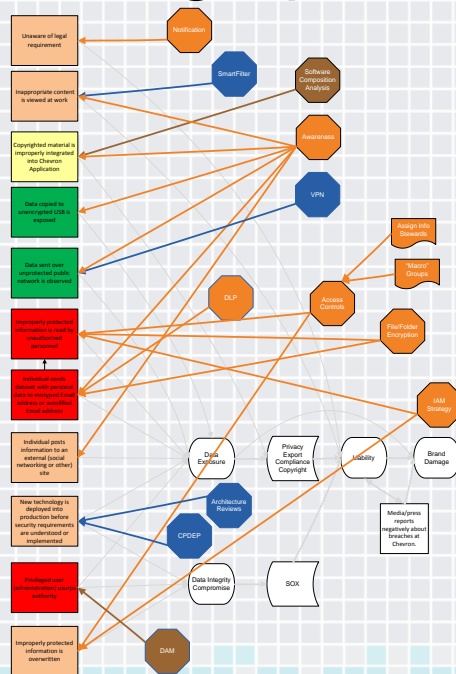


Scenario modeling

◆ Threat modeling

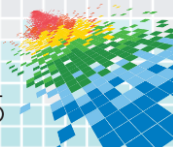
Attacker	Tradecraft	Vulnerability	Action	Target	Result	Objective
Nation State - high motive, high capability	Advertise wrong BGP Routes	Excessive/improper access	Spoof	Ports	Theft	Financial Gain
Nation State - high motive, low capability	Cable physically severed	User behavior	ReRoute	People	Data loss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

◆ Attack graphs



Threat modeling

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



Threat modeling – Example One

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



Threat modeling – Example Two

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



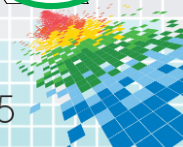
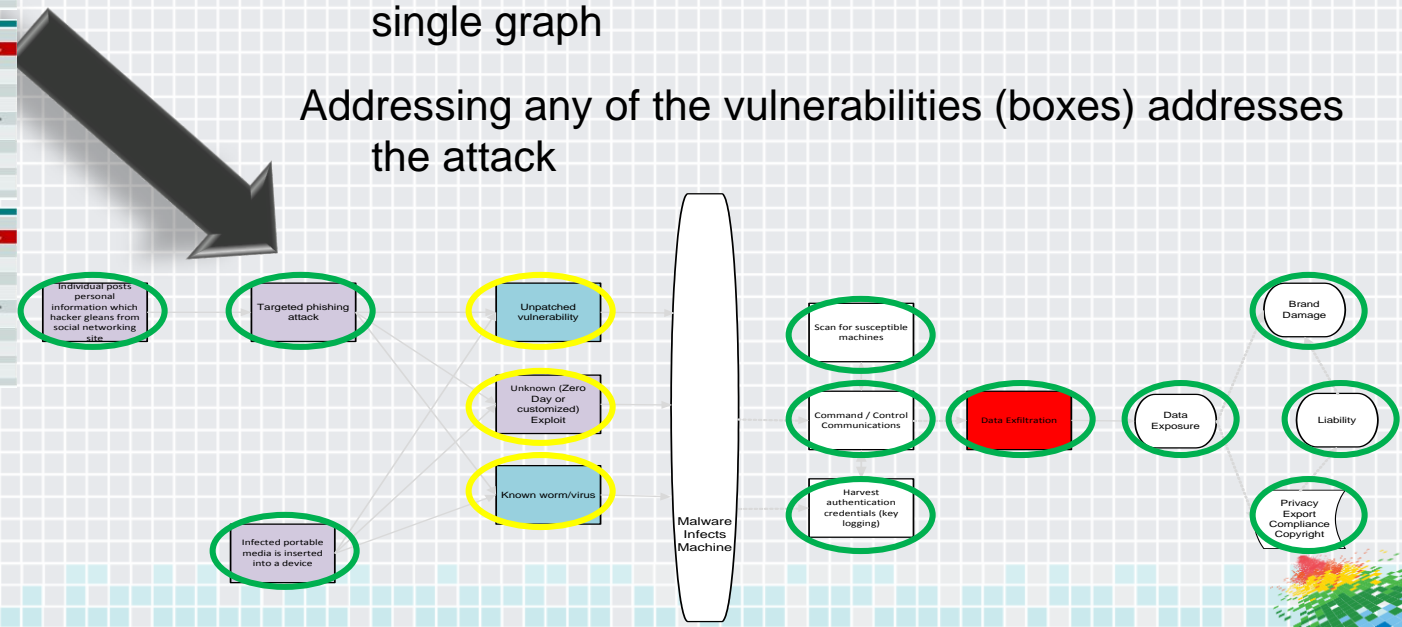
Attack Graphs

Exploit	Vulnerability	Exploitation	Attack	Target	Result	Consequence
RemoteExec - High privilege, high capability	RemoteExec RFP needs	RemoteExec remote access	local	File	Conf	Compromise
RemoteExec - High privilege, low capability	Local physical access	User behavior	Remote	People	Data loss	Confidentiality breach
RemoteExec - Low privilege, low capability	OS vulnerability	Denial of service	Local	IT infrastructure	Control	Strategic advantage
RemoteExec - Anonymous	OS Vulnerability (of service)	Privilege escalation	Local	OS user	Denial of service	Malware
RemoteExec - Confidential	OS vulnerability	User interaction	Remote	IT infrastructure	Operational damage	Strategic advantage
RemoteExec - Information gathering	OS vulnerability	Remote systems	Remote	Control plane	Abuse of trust	Service compromise
Operational	OS function	Informational data	Local	Control plane	Deny	Informational breach
Malware/inject	Cross-site scripting	Session application management	Deny	Key	Denial of service	Control
RemoteExec - Inheritor (local)	RemoteExec	Open vulnerabilities	Identify threat	Code/data	Regulatory investigation	Control
Malware/primitive user (admin/monitor)	Malware	Malware	Malware	Malware	Malware	Malware
	Physical access	Physical access (user/business)	Physical access	Physical access	Physical access	Physical access
	Social engineering	Social engineering	Social engineering	Social engineering	Social engineering	Social engineering

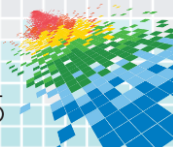
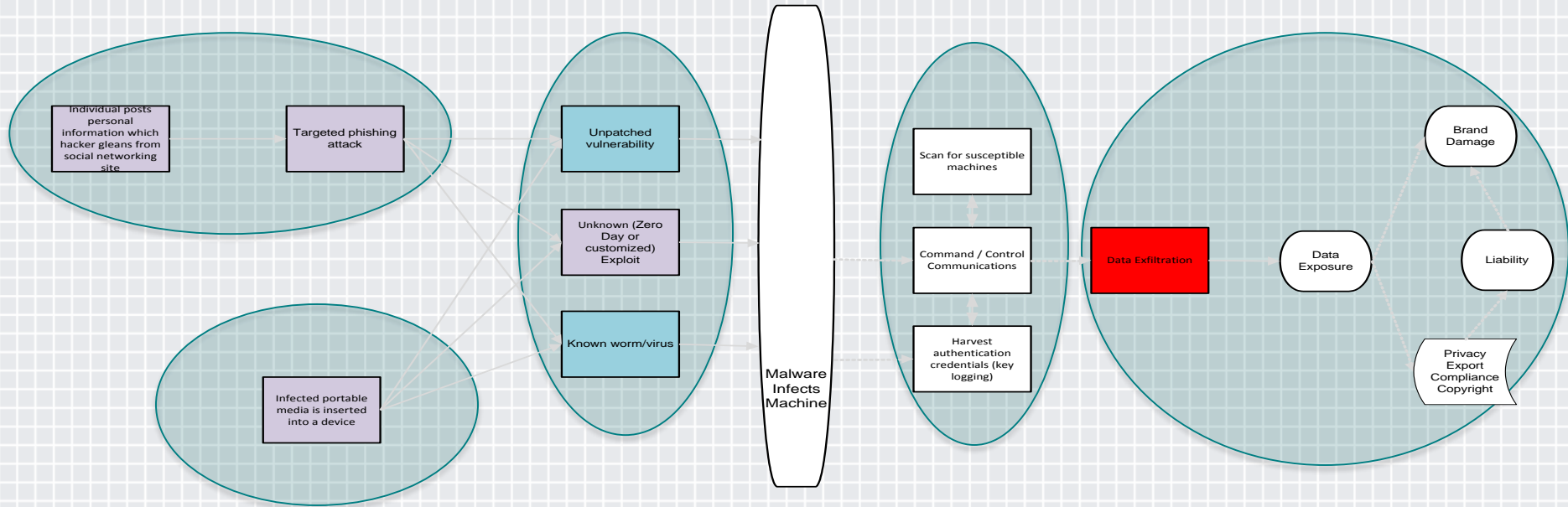
Visual representations of possible attack paths and consequences

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

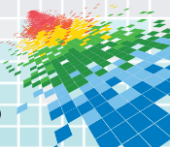
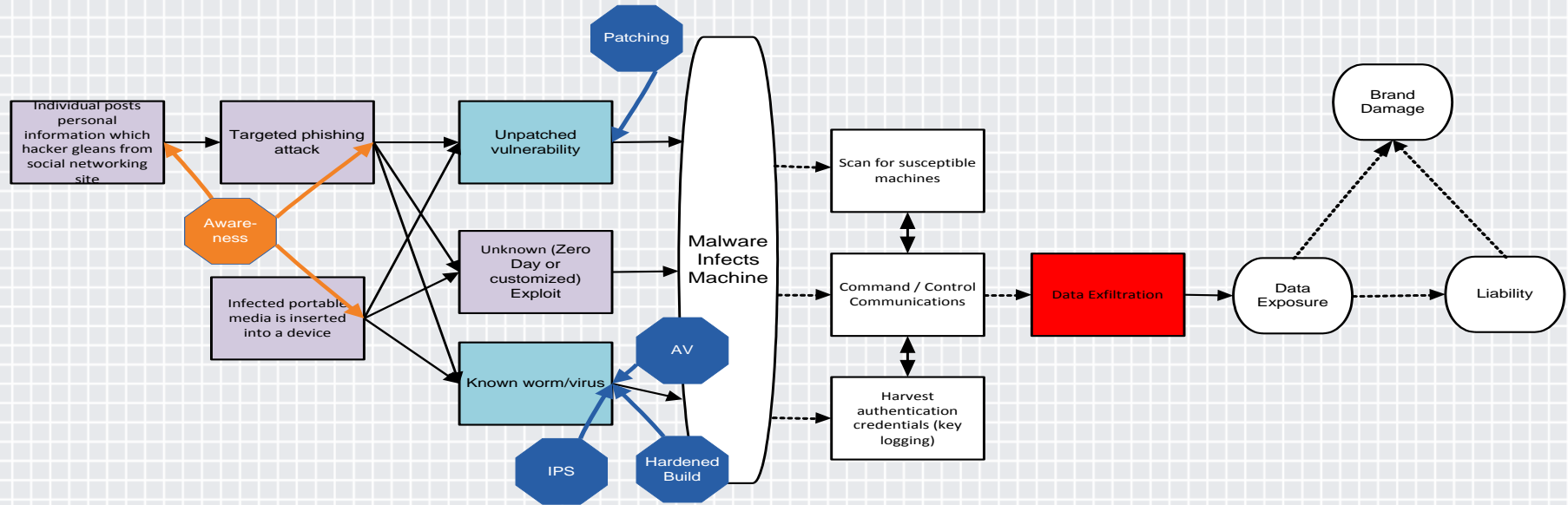
Addressing any of the vulnerabilities (boxes) addresses the attack



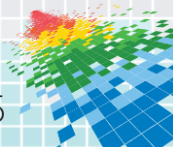
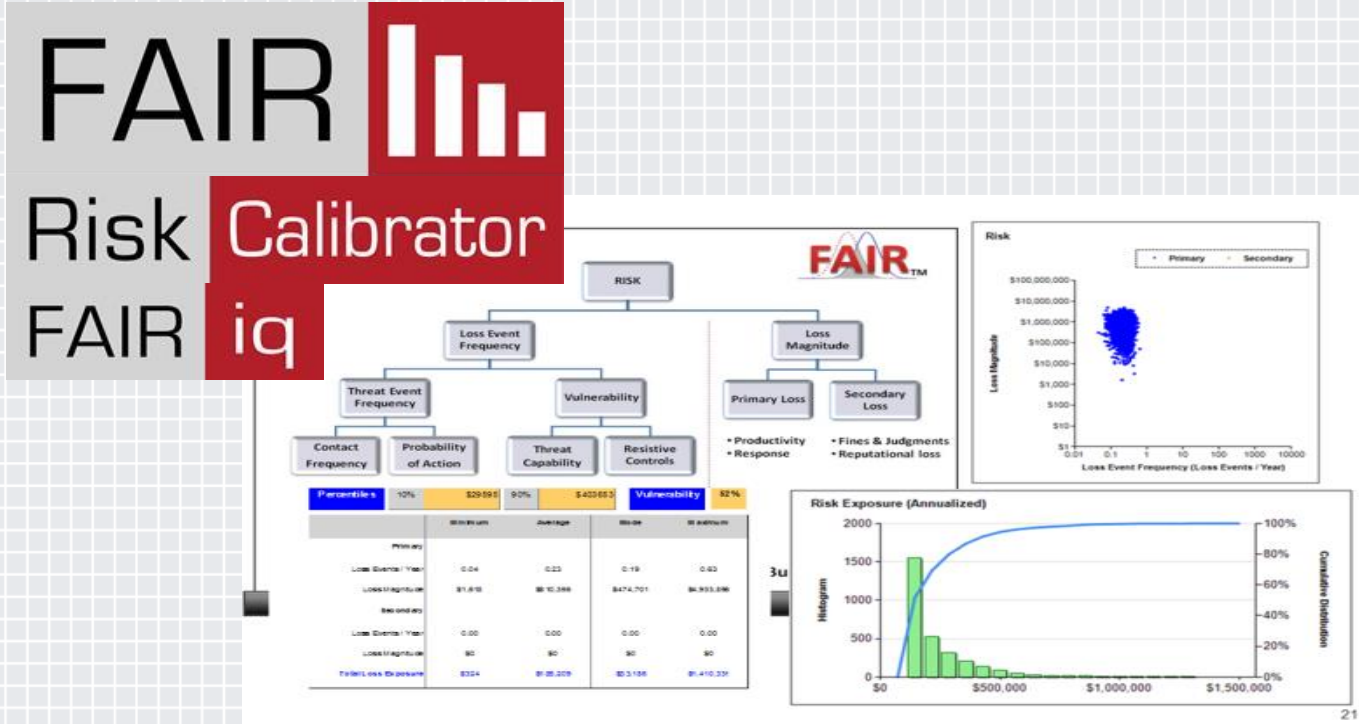
Addressing APT: A typical targeted attack



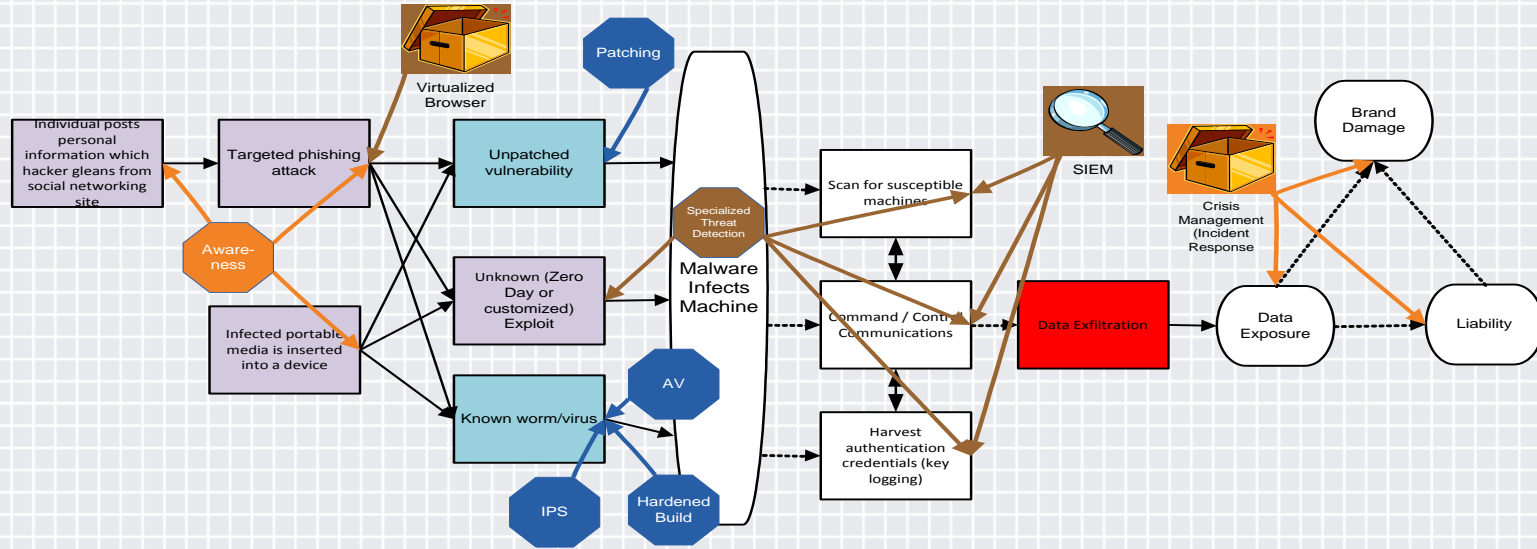
Current Control Set Versus APT



Quantitative Risk Assessment



Putting it all together – Addressing APT



Maintain

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

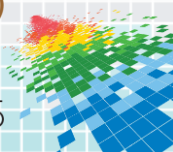


Maintain and Improve

- Awareness training
- Incident response (implement crisis management)

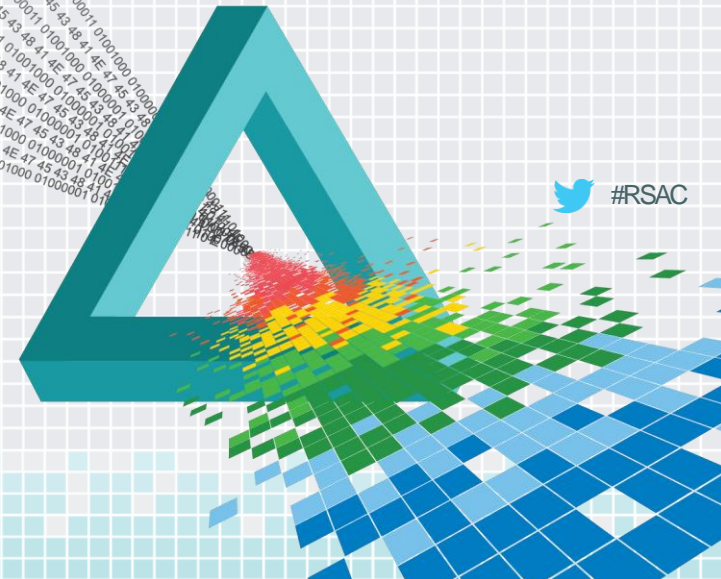
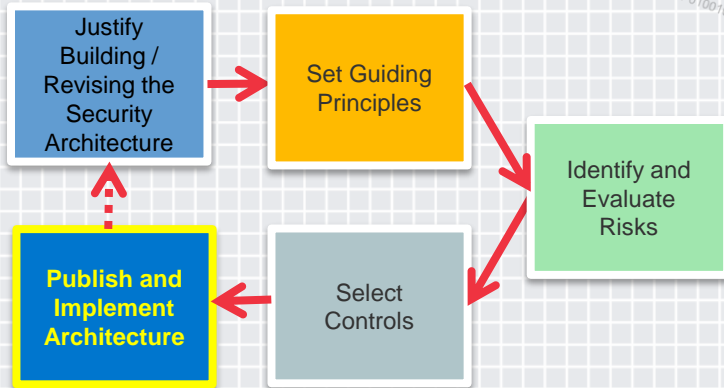
Implement

- Virtualized browser
- Specialized Threat Detection
- SIEM (Security Information and Event Management)

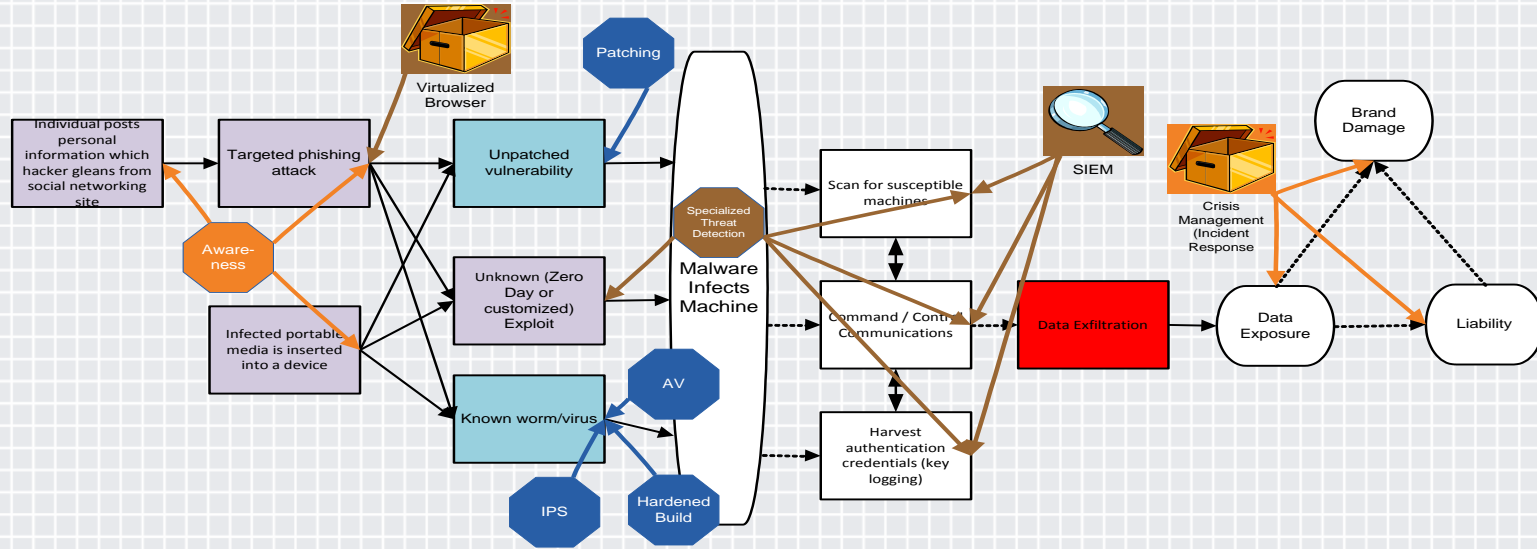


RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center



Optimizing risk reduction with budget



Maintain

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

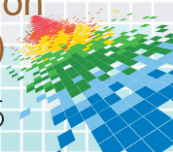


Maintain and Improve

- Awareness training
- Incident response (implement crisis management)

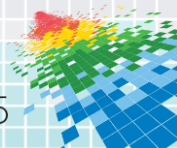
Implement

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



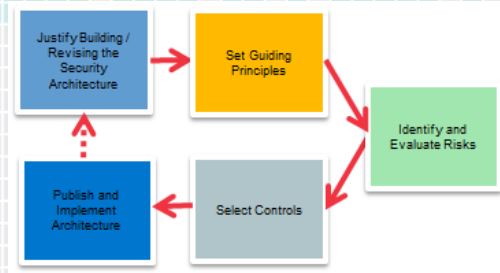
Where we are going...

- ◆ 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

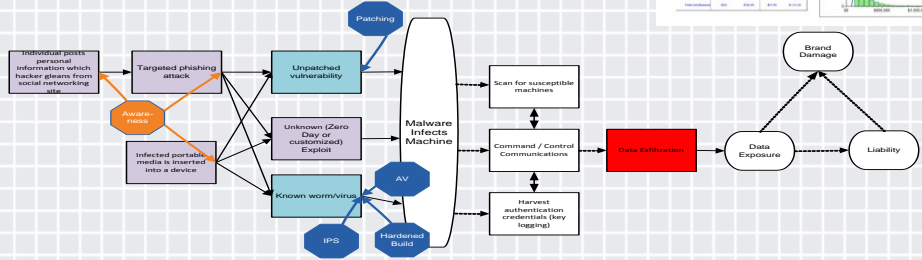
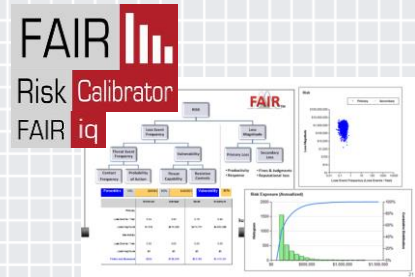


Apply Slide

- ◆ 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



Category	Control	Control	Control	Control	Control	Control
Network	Network segmentation	Network segmentation	Network segmentation	Network segmentation	Network segmentation	Network segmentation
Application	Application whitelisting	Application whitelisting	Application whitelisting	Application whitelisting	Application whitelisting	Application whitelisting
Endpoint	Endpoint protection	Endpoint protection	Endpoint protection	Endpoint protection	Endpoint protection	Endpoint protection
Identity	Identity management	Identity management	Identity management	Identity management	Identity management	Identity management
Access	Access control	Access control	Access control	Access control	Access control	Access control
Logging	Logging and monitoring	Logging and monitoring	Logging and monitoring	Logging and monitoring	Logging and monitoring	Logging and monitoring



Resources

◆ Threat Modeling

- ◆ John Howard, Thomas Longstaff; “*A Common Language for Computer Security Incidents*”; Sandia National Laboratories; October 1998. DOI= <http://prod.sandia.gov/techlib/access-control.cgi/1998/988667.pdf>

◆ Attack Graphs

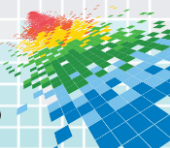
- ◆ Anoop Singhal, Ximming Ou; “*Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs*”; National Institute of Standards and Technology; August 2011. DOI= <http://csrc.nist.gov/publications/nistir/ir7788/NISTIR-7788.pdf>
- ◆ Ian Green “*Extreme Cyber Scenario Planning and Attack Tree Analysis*”; Commonwealth Bank of Australia – presented at RSA Conference 2013; Video - <http://www.rsaconference.com/media/extreme-cyber-scenario-planning-fault-tree-analysis>; Slides - http://www.rsaconference.com/writable/presentations/file_upload/stu-w21b.pdf

◆ Scenario Planning

- ◆ Peter Schwartz; “*The Art of the Long View: Paths to Strategic Insight for Yourself and Your Company*”; Currency Doubleday; 1991
- ◆ “*Scenarios: An Explorer’s Guide*”; Shell International BV; 2008; <http://s05.static-shell.com/content/dam/shell/static/future-energy/downloads/shell-scenarios/shell-scenarios-explorersguide.pdf>

◆ Risk Assessment

- ◆ The Open Group™ Risk Taxonomy Standard (O-RT): <https://www2.opengroup.org/ogsys/catalog/C13K>
- ◆ The Open Group™ Risk Analysis Standard (O-RA): <https://www2.opengroup.org/ogsys/catalog/C13G>



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: ANF-W03R

Questions?

Michael J. Lewis

Senior Staff Security Strategist

Chevron

Michael.J.Lewis@chevron.com

CHANGE

Challenge today's security thinking

