Cyber Security Challenge

ISSA Symposium

TJ Harrington
Managing Director
Chief Information Security Officer
Challenging Threat Landscape

- Third Party Compromise
- Ransomware
- Organized Cyber Crime
- Malware
- Data Breach
- DDoS
- Mobil Attacks
- Nation State
- Espionage
- Technical Vulnerabilities
- Insider Threats
- Influence Ops
- Malware Attacks
What Do Your Devices Know About You?

- Passwords
- Fingerprint
- Credit Cards
- Recent Locations
- National ID
- Recently Visited Sites
- Phone Calls Placed
- Your Name & Address
- Current Location
- Recent Locations
- Purchase History
- Deleted Files
- Bank Account Information
- Contact Lists
- Text Messages
- Pictures of Family & Friends
The Challenge Before US

- Cyber Crime delivers a higher return on investment than the drug trade
- Low barriers to entry for criminal actors, the face little to no prospect of prosecution or punishment.
- Crime-As-Service grows with expanded tool sets and services.

- Governments globally recognize cyber as a tool of espionage, a “first strike” weapon in warfare and a unique leveler between world powers and emerging states.
- Regulations are adding a complexity to critical asset management. A lack of harmonization, conflicts in standards, global protectionist steps and government’s failure to create cyber deterrent strategies are at the center of the challenge.

- Cyber attacks increase, so does awareness, the result is a war for talent to find a skilled workforce to build cyber defense teams.
How easy is it for the adversary to gain a foothold in your organization?

95% of Successful Attacks Begin with a Phishing Attack

So let’s see how it can happen
Cyber Attacks – Historical Perspective

- **2013**: Iranian DDOS Attacks Against U.S. Financial Sector
- **2014**: Target
- **2015**: Sony, J.P. Morgan
- **2016**: Sands, Anthem, Ashley Madison
- **2017**: Yahoo!, FedEx, Maersk, Merck, Uber
- **2018**: Equifax, LinkedIn

*ISSA*
How Confident is your team that they are prepared for a bad day?

75% of IT Professionals responded that they did not have a formal cyber security incident response plan.

66% of those respondents were not confident in their ability to recover from an attack

Cost of a Data Breach in 2017 was $7,350,000

Source: IBM & Ponemon 2017 Survey of 2,400 IT Professionals.
Recent Major Cyber Attacks


- Global attack targeting Microsoft operating systems XP and Windows 7
- Over 300,000 computers infected in 150 countries
- UK NHS (70k devices), Telefonica, FedEx, Deutsche Bahn, Nissan, Renault
- Most impacted countries: Russia, Ukraine, India, and Taiwan
- Cost estimates: Hundreds of millions to $4 billion U.S. dollars

“Petya/Not-Petya”: June 2017

Global attack targeting MS Windows systems using Ukrainian tax program M.E. Doc

- Appeared to be a ransomware attack but actually destroyed data
- 80% of infections in Ukraine, with others in Germany, France, Italy, Poland, UK, USA

Impacts include:
- Radiation monitors in Ukraine’s Chernobyl nuclear power plant went offline
- Ukrainian ministries, banks, and metro systems shut down
- India’s largest container port shutdown
- Maersk reported up to $300 million U.S. dollar revenue loss
- FedEx 10-K SEC filing reported “material impact(s)”
- W.V. Princeton Hospital completely replaced computer systems
Cyber has become their solution by blending Military/Criminal operations using nation-state resources:

- SWIFT
- Wannacry
- ATMs
- DDoS
- Espionage

- Cryptocurrency
- Banks
- Media
- Government
- Opportunities

...but they need to monetize their take
Today most cyber adversaries are people; people who represent a reasoning actor, one who weighs means and ends, costs and benefits and makes a rational choice.

With the right strategy and successful execution you can influence the choice made by an adversary.

First Step Think Like An Attacker
Do you have a comprehensive cyber strategy?

Is your strategy built on a sound, recognized standard?

**Control Defense**
- Hygiene Controls
  - (Firewalls, Patch Mtg, Antivirus, Scanning & Monitoring)
- Data Protection
- Identity & Access
- Third Party Management
- Application Security
- Privileged User Management
- SIRT Management
- Infrastructure

**Active Defense**
- **Intelligence Operations**
- Information Sharing
- Deception & Denial
- Honey Pots & Sandbox
- Hunting
- Vulnerability Assessment Team
- Playbooks
- War Gaming
- Coordinated Disrupt Ops
- Beacons on Data

**Offense**
- Hack Back
- Rescue & Recovery
- Civil Law Suits
Are you prepared for a Bad Day?

- Commander’s Intent Statement
- Clarity on Command & Control Functions
- Clarity on Decision Rights
- Alignment with your Crisis Management Team
- Have you practiced your response?
Cyber Crisis Management

- Develop a Cyber Crisis Management Framework: provides unique role overviews for holistic response
- Integrated with your crisis communications technology and processes
- Provides pre-planned action options meant to contain cascading impacts, but may also result in business impact
- Pre-defines containment option decision makers, execution protocols and key communications considerations
- Equipped with specific checklists for all global teams to ensure intelligence gathering, analysis and operational needs are completed in a thorough and thoughtful manner
Proposed Immediate Action Model

Need to Contain in 0 – 60 Minutes

High Risk, High Consequence Cyber Attacks

Used only if a Cyber Crisis Event or Incident has become Significant or Catastrophic and time is of the essence for response.

EO&T responds initially for all of the company with others joining as soon as possible.

0 MIN 5 10 15 20 25 30 35 40

60 MINS 24 HRS 48 HRS Closure

0 – 60 Respond

Validate - Stabilize - React/Respond

45 – 60 React

EO&T

B-1  B-2  NAM  LATAM  EMEA  ASPAC

GPA  Legal  Risk  Compliance  CBNA
Cyber Leadership Truths

Trust is built over time - it cannot be surged at a time of need

The more you sweat in practice, the less you will bleed in battle

You can predict the future if you can shape the future

Talent - Teamwork - Technology