Top Cybersecurity Threats in 2017

- Dr. Bader Al-Manthari
- Information Security Division (ISD), ITA
- 26/01/2017
Agenda

- Top Cybersecurity Threats
  - False Sense of Security
  - Misaligned Security Spending Strategy
  - Cyber Physical Convergence
  - Work Life Convergence
  - Insider Threat
  - Rise of Financially Motivated Attacks
  - IoT-based DDOS Attacks
  - Rise of “Simple” Breaches

- Recommendations
False Sense of Security

- Having a firewall and antivirus does not necessarily mean that you are secure

- Security is a complete program consisting of clear support and direction from top management, processes, policies, technologies, and people

- Any issue in any of these components will expose the organization to security risks
Misaligned Security Spending Strategy

- Only **38%** of organizations have a methodology to prioritize security investments based on greatest risk to the business*

- **17%** classify the business value of data*

* PWC
86% of security spending*

* HP
Misaligned Security Spending Strategy

- Security breach is inevitable
- Almost half of the organizations do not have an incident response plan*
- 146 day average time to detect a breach**
- Since 2009, time to resolve an attack has grown by 130% ***
- Only 23% conduct cyber threat analysis****
- How much is spent on staff training and awareness?

*Threat Track Security
** FireEye
**** HP
*** PWC
Cyber Physical Convergence

- Many industrial control systems increasingly relay on ICT which expose them to great risks

- Power Plant Hacking in Ukraine*

- Airplane hacking**

- Aurora Generator Test**

- Hacking of Jeep Cherokee ***

* WeLiveSecurity
**CNN
***Wired
Cyber Physical Convergence

- Hacking of a water utility’s control system*

- Hacking of health equipment

- Hacking of Iranian Nuclear Plant**

- Cyber Attacks will cause human casualties before 2025***

- Legal consequences of cyber physical convergence

*The Register  
**Business Insider  
***Pew
Cyber Physical Convergence

Confidentiality

Integrity
Availability
Cyber Physical Convergence

Confidentiality

Safety

Integrity

Availability
Work Life Convergence

- Segregation between work and life has become difficult
- Employees increasingly demand to use their own devices at work
- Work Life Convergence
  - Bring Your Own Device (BYOD)
  - Social Media
  - Internet of Things
Work Life Convergence (Bring Your Own Device)

- Greatest risk with BYOD is the inability to control the personal devices connected to the organization’s resources
- 85% of organizations allow their employees to use personal devices at work*
- 67% of employees use their personal devices at work regardless of the BYOD policy**

* IDG Research Services
**Microsoft
Work Life Convergence (Bring Your Own Device)

- 77% of employees have not received any security awareness regarding BYOD*

- By 2018, 70% of mobile users will conduct work from their mobile devices**

- 80% of personal devices are not managed by the organization***

*AllThingsD  
**Gartner  
*** SecureEdge Networks
Work Life Convergence (Social Media)

- 52% of adults connected to the Internet use one or two social media sites*
- 70% of active Internet users use social media**
- 90% of adults between 18 and 29 use social media*
- 75% of users use the same password for social media and their email

*Pew Research
**Link Humans
***Zerofox
Work Life Convergence
(Social Media)

- 70% of social media risks were shared by the users themselves in 2014 compared to 2% in 2013*

- 40% of social media users accept friendship requests from people they don’t know*

- 78% of burglars admitted to use social media to select their targets**

- 15% of Americans feel that share everything or most things on social media***

*Symantec
**Friedland
***Washington Post
Work Life Convergence (Internet of Things)

- **200** Billion device connected to the Internet by 2020*

- **26** smart device for every person on earth by 2020*

- **90%** of the cars will be connected to the Internet by 2020**

- **47%** of organizations expect the number of IoT devices on their networks to increase by at least **30%** in 2017***

- First IoT attack detected in 2014****

---

*Intel  
**Telefonica  
***Tripwire  
****Proofpoint
Work Life Convergence (Internet of Things)

- 90% of connected devices collect personal information*
- 70% of connected devices send information in plain text*
- 70% of common IoT devices contain vulnerabilities*
- 152% increase in breaches of IoT devices connected to the cloud in 2015**

*HP
**PWC
Work Life Convergence (Internet of Things)

Is Your Organization Ready to Deal with the Risks of IoT?

Source: Ponemon Institute, 2015 Global Megatrends in Cybersecurity
The Insider Threat

- Most of the dangerous attacks come from the inside
- Malicious insiders/Human errors
- Staff turnover and Disgruntled employees
- 93% of investigated incidents in 2014/2015 where because of human errors*
- 2/3 of government data breaches are accidental leaks**

*Information Commissioner's Office  
**Symantec
The Insider Threat

- Awareness and Training
- Social Engineering
- Work Life Convergence
- Information Security Leadership
89% of C-level executives feel that their organizations are vulnerable to the insider threat*

43% of IT managers think that employees’ negligence poses the greatest risk to sensitive data**

58% keep sensitive data on their mobiles***

91% detected employee abuse of Internet access privileges****

*Vormetric  
**Ponemon  
***EMA  
****InfoSight
The Insider Threat (Awareness and Training)

Does Your Organization Need More Knowledgeable and Experienced Cybersecurity Practitioners?

- US: 67%
- UK/Europe: 66%
- MENA: 65%

Source: Ponemon Institute, 2015 Global Megatrends in Cybersecurity
The Insider Threat
(Awareness and Training)

- 56% of corporate employees have not taken security awareness training*
- 42% of organizations spend less than 1% of their security dollars on awareness programs**
- 63% of organizations that provide security awareness training for their employees, provide less than 5 hours of training per year**

*EMA  
**InfoSight
The Insider Threat (Social Engineering)

- **55%** increase in Spear-Phishing Campaigns Targeting Employees*
- **91%** of cyberattacks start with a phishing email**
- **85%** of organizations have suffered phishing attacks
- **#1** delivery vehicle for ransomware and other malware is email attachment ****

*Symmantec  **PhishMe  ***Wombat  ****Verizon
The Insider Threat
(Social Engineering)

- **1 in 3** companies have been victims of CEO fraud emails*

- **90%** of the people provide not just the spelling of their names but their email addresses without confirming the requester’s identity**

- **67%** of the people give out social security numbers, birthdates or employee numbers**

- **100%** success ratio in physical breaches**

---

*AlienValut
*Social-Engineer, Inc
Information security leaders are generally technical leaders not business leaders.

They are not able to speak the language of their top management.

Information security doesn’t get the right attention from top management.

Information security budget is not spent smartly to address business risks.
The Insider Threat (Information Security Leadership)

Which is the biggest skill gap you see in today’s security professionals?

- Technical skills: 390 (46.32%)
- Ability to understand the business: 609 (72.33%)
- Communication: 355 (42.16%)

Total Respondents: 842

Does senior leadership view cybersecurity as a strategic priority?

Source: Ponemon Institute, 2015 Global Megatrends in Cybersecurity
Does your organization’s security leader brief the board of directors on the cybersecurity strategy?

Source: Ponemon Institute, 2015 Global Megatrends in Cybersecurity
Do you agree C-level executives and boards of directors are fully briefed about security priorities and required investments?

Source: Ponemon Institute, 2015 Global Study on IT Security Spending & Investments
The Insider Threat (Information Security Leadership)

What best describes your organization’s approach to determining the IT security budget?

- Senior management determines the budget: 39%
- The budget is based on an assessment of our organization’s security risks: 32%
- The budget is based on what the organization feels is the right amount: 15%
- The budget is a set percentage of the total IT budget: 12%
- Other: 1%

Source: Ponemon Institute, 2015 Global Study on IT Security Spending & Investments
Rise of Financially Motivated Attacks

- **35%** increase in ransomware attacks in 2015*

- **93%** of all phishing emails contained ransomware**

- Provided as a service (Ransomware-as-a-service)

- **Targeted Ransomware**

*Symantec  
**PhishMe
Rise of Financially Motivated Attacks

Source: Verizon, 2016 Data Breach Investigation Report
Rise of Financially Motivated Attacks

Attacks on KrebsOnSecurity.com, OVH, and Dyn

In the past botnets were comprised of actual computers

47% of organizations are concerned about the weaponization of IoT devices for DDoS attacks*

Hackers can shut down the organization online capabilities

Use IoT-based DDOS attacks as a cover hide another attack (data breach)

*Tripwire
Many organizations’ security is so lousy that hacking doesn’t require actual hacking”*

63% of confirmed data breaches involve leveraging weak/default/stolen users and passwords**

30% of phishing messages were opened by the targets**

Through 2020, 99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year***

Work life convergence and the insider threat will increase the percentage of “simple” breaches in the future

*Quartz  
**Verizon  
***Gartner
Recommendations

- Organizations Must commit to protect their valuable information assets

- Create a culture of valuing and protecting information
  - Strong management leadership and commitment
  - Responsibility of everyone for protecting information
  - Extensive awareness, training and education

- Focus on the human aspects and put emphasis on education, awareness, and training

- Focus on information security leaders within the organization
Recommendations

- Address cyber security holistically using a risk-based approach
- Ensure that your spending on cyber security is strategically aligned with the overall business strategy
- Beware of data supply chain risks
- Improve visibility within the organization and focus on incident detection and response
- Need to share threat intelligence with other organizations
Thank You