Systemic Cyber Risk and Exposure of the Insurance Industry

Ron Bushar, VP, FireEye Professional Services
Christopher Porter, Chief Intelligent Strategist
The Problem

Offense
- Melissa
- CodeRed
- Spam
- Spyware
- Trojans
- Worms, Bots
- Zero-days
- Rootkits
- APTs
- Phishing
- Ransomware
- Mobile Threats
- IoT Threats

Defense
- Anti-spam
- URL Filtering
- Data Loss Filtering
- Whitelisting
- Anti-malware
- Heuristics
- Behavioral Analysis
- Detonation Chambers
- Intelligence
- Orchestration
- Automation

1990s
- Opportunistic

2000s
- Targeted

2010s

Today
How Good Do You Need To Be?

Security Capability

Sophistication of the Threat

Tools-Based

Integrated Framework

Adaptive Defense

Resilient

Organized Cybercrime

Compliant

Standard Cybercrime

Conventional Threats

Security Capability
Background: Why Cybersecurity Risk Management?

Old methods don’t work

Need to engage at Board-level

Rapid growth in cyber insurance market

What factors make it easier/harder to convey value?


Expectation globally, by 2022, a 28% CAGR from 2016 – 2022.

$14B
Risk Services Objectives

◆ Help the CISO / CIO communicate business risk at the Board-level.
◆ Help client security operations use risk management techniques in practice.
◆ How do you communicate the scale of the risk to stakeholders across the team?
◆ What organizational steps does your team use to reduce risk?
  ▶ Examples - mapping key assets and putting contingency plans in place.
◆ How can you financially transfer these risks?
Intelligence-led security is about risk management

◆ What should organizations be doing to benefit from intelligence-led security?
◆ Companies need real-time adversary analysis before an incident.
◆ Understanding the risks, what informational assets (and asset value) an organization has, and where those assets are located.
◆ Who at the company is responsibility for assessing and mitigating breach-related risks? Not just the chief information security officer (CISO).
◆ Cyber Team should consist of internal stakeholders as well as outside partners like law firms, insurance experts & Forensic teams like Mandiant.
Defining your risk impact across the organization

Cyber is not just an IT issue.

It is an enterprise risk that impacts many key stakeholders within your organization.

CYBER RISK: EVERYONE HAS A STAKE
Where should I start?

◆ Incident response plans?
◆ Has your team done a table-top exercise?
  ▶ Both technical & executives should participate.
◆ Practice and include your outside partners.
  ▶ This is a working document, so update the plan after practice.
◆ Once you’ve identified gaps, create action plans to eliminate them.
Breach Response Hot Topics

- Having a communications playbook
- Dealing with Brian Krebs
- The right mitigation product (credit monitoring and others)
- The “b” word
- Notification timelines & expectations
- Your plans (not just Incident Response plans)
- Breach response goals vs. risks
Achieve Resilience by focusing on the “Relevant Threats”; “Buy Down” Cybersecurity Risk by Optimizing Investment in Countermeasures

How does the adversary view your organization?

Transformed Services

- Cyber Defense Center
- IR Retainer
- Cyber Threat Intelligence Services (CTIS)
- Table-top Exercise
- Industrial Control Systems
- Managed Defense
- FireEye iSight Intelligence

Products

- FireEye Helix
- FireEye Threat Analytics
- FireEye Network Security
- FireEye Endpoint Security
- FireEye Email Security

Identify & Track the “Relevant Threats”

Assess attack surface & cyber defense capabilities

Measure business risk & plan investments

Harden attack surface

Services

- Threat Diagnostic
- Compromise Assessment
- CTIS Threat Profile
- Response Readiness Assessment
- Security Program Assessment
- M&A Assessment
- Pen Testing & Red Team
- Risk Services

Optimize decision-making with risk-led security
Identify & Track the “Relevant Threats”

Use threat diagnostics or iSight Intelligence to inform and guide.

What are the “Relevant Threats” to your Organization?

- Cyber Espionage: Motivation: Strategic Advantage
- Cyber Crime: Motivation: Financial Gain
- Hacktivism: Motivation: Ideology

Your Organization
- Line of Business 1
- Line of Business 2
- Line of Business 3
- Line of Business 4
- Line of Business 5
- Line of Business 6
Measure Business Risk and Plan Investments

**Old Method**
Reliable measures of risk cannot be derived from a simple equation...

Probability × Impact
× Vulnerability = Risk

**New Method**
Optimize by relying on risk models appropriate to your organization. Allow for inclusion of multiple risk factors.

- Threat
- Capability
- Countermeasure
- Strength
- Threat Frequency
- Value at Risk
- Risk Models

©2018 FireEye | Private & Confidential
2018 and beyond...

- More destructive attacks
- Attribution will become more important
- Attacks will continue to align with global conflicts
- More reliance on cloud infrastructure (both victims and attackers)
- Cybersecurity will continue to be a national focus
- More and more sophisticated threat actors will emerge
- More government involvement
- Intelligence and sharing are critical to stay ahead of the threats
- Attacks against safety control systems
Insurance a Top Finance-sector Target

**Detected Activity by Subsector**

- **Banks & Credit Unions**: 72
- **Invest**: 24
- **Insurance**: 21
- **Credit Cards**: 8
- **Exchanges & Trade**: 4
- **Brokerages**: 3
- **Lend**: 7
- **Realestate**: 8

©2018 FireEye | Private & Confidential
Investment Targeting by Actor

- APT1: 32%
- APT19: 5%
- APT29: 5%
- APT33: 5%
- APT34: 5%
- FIN4: 5%
- FIN7: 5%
- FIN9: 5%
Thank you.
We look forward to working with you.