Managing Security Risk

Steven Leo
IBM Security Services

IT Security threats - many sources and many ways.

1. Number of Attacks have increased Significantly
2. Sophistication of attacks have become more complex
3. Lack of IT Security skills in the industry contributing to security risks
4. Security incidents increasing effect corporate reputation/brand

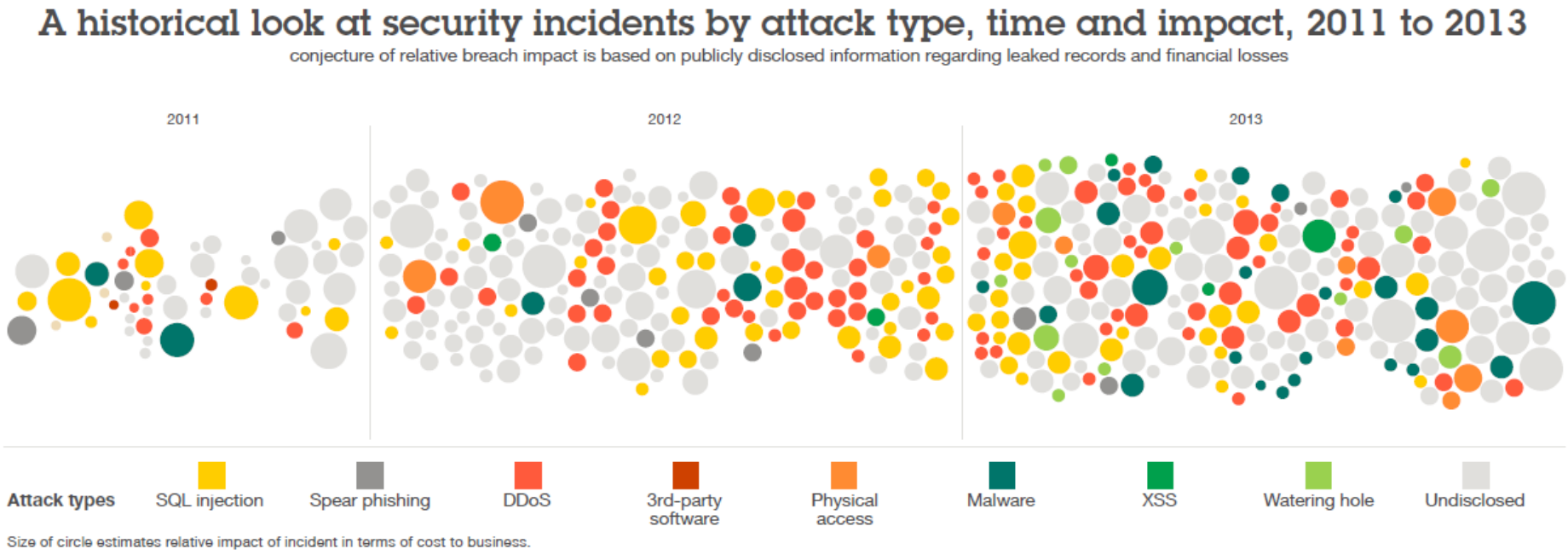


Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

The new security landscape

Increased connectedness introduce vulnerability

Digital Interconnectedness

- Embedded systems
- Globally interconnected networks

Anywhere, Anytime Access

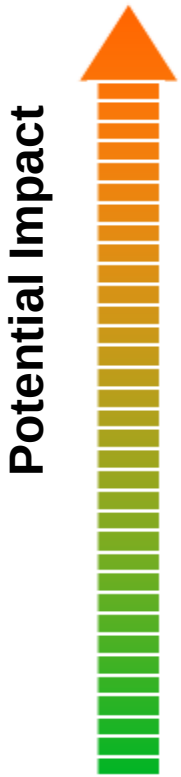
- Mobility
- “Bring-Your-Own Device”
- Social business

Pervasive Data

- Big Data analytics
- Consumer applications

The new security landscape

Sophisticated attackers are a primary concern

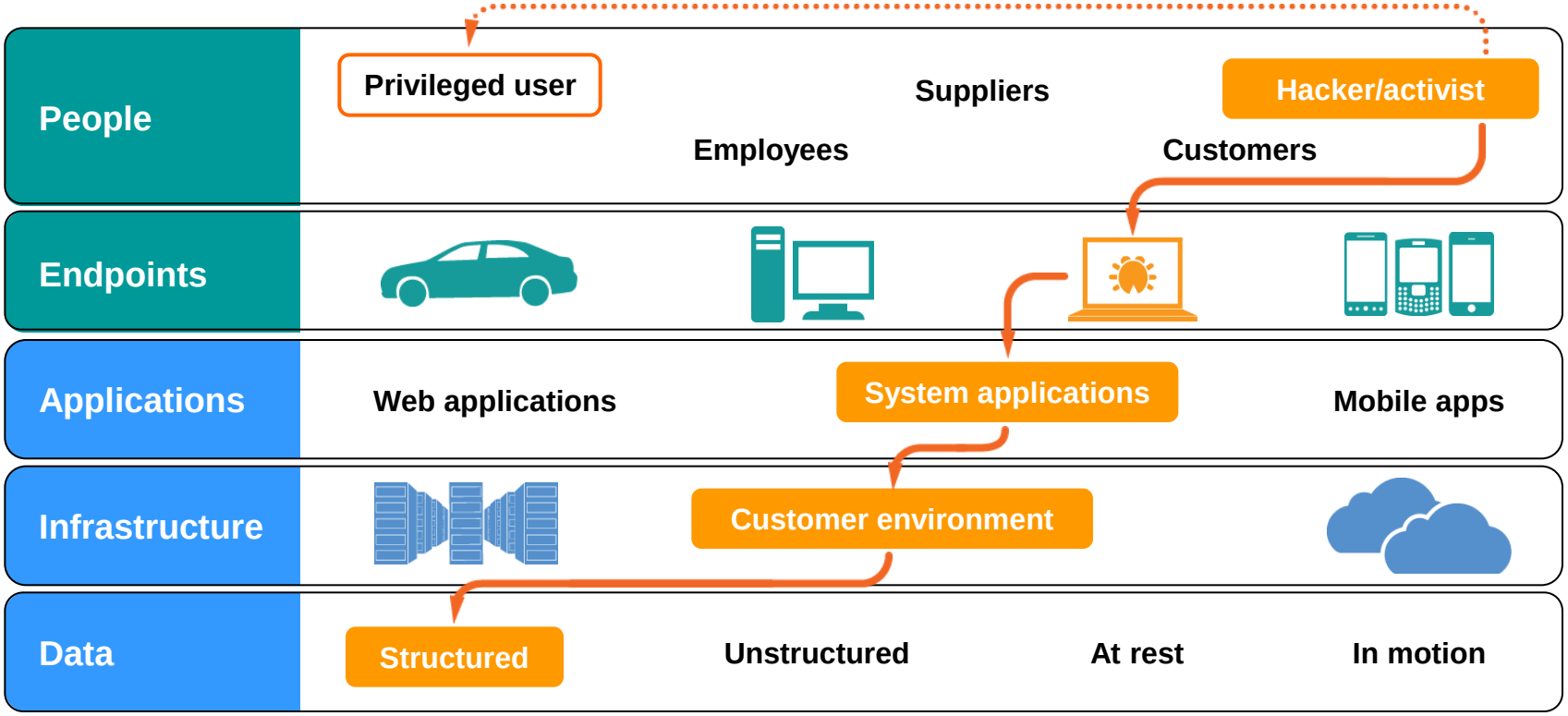


Threat	Profile Type	Share of Incidents	Attack Type
Advanced, Persistent threat / mercenary	▪ National governments ▪ Terrorist cells ▪ Crime Cartels	23%	▪ Espionage ▪ Intellectual property theft ▪ Systems disruption ▪ Financial Crime
Insiders	▪ Employees ▪ Contractors ▪ Outsourcers	15%	▪ Financial Crime ▪ Intellectual Property Theft ▪ Unauthorized Access/
Hacktivist	▪ Social Activists	7%	▪ Systems disruption ▪ Web defacement ▪ Information Disclosure
Opportunist	▪ Worm and virus writers ▪ “Script Kiddies”	49%	▪ Malware propagation ▪ Unauthorized Access ▪ Web defacement

Source: Government Accountability Office, Department of Homeland Security's Role in Critical Infrastructure Protection Cybersecurity, GAO-05-434; IBM CyberSecurity Intelligence & Response Team, September 2012

The new security landscape

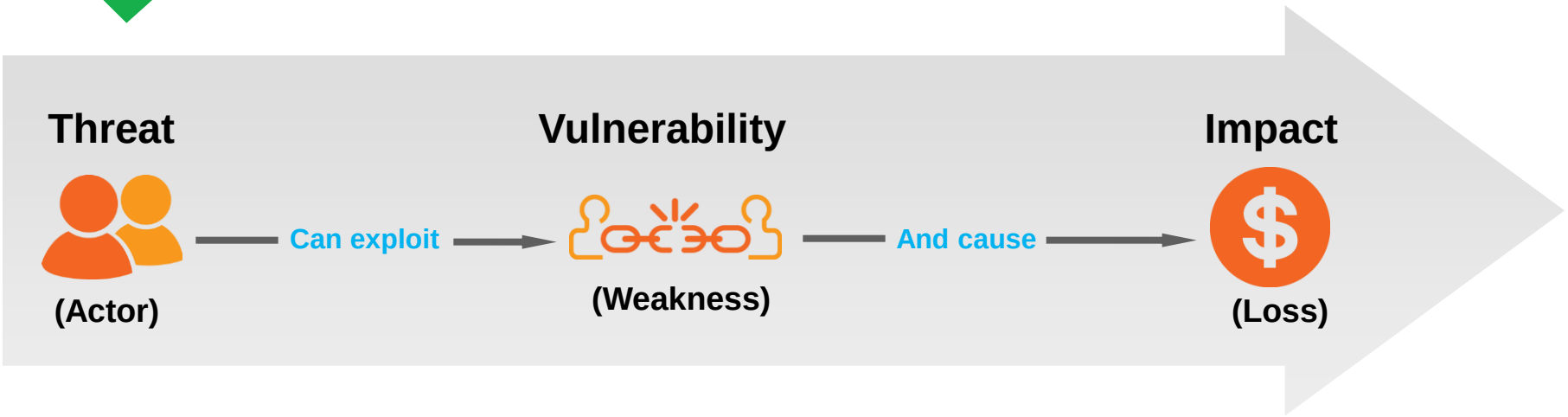
Representative customer case study of a sophisticated attack



- Adversary compromises endpoint used by privileged user with undetectable malware
- Keystroke logger capture credentials and command & control capability is gained
- Adversary acts as systems administrator
- Data is stolen and/or production systems are compromised

To stay ahead we focus on disrupting the attacker's capability, timeline and impact

Security risk exists when …



Security Risk Management is the application of **control** to detect and block the threat, to detect and fix a vulnerability, or to respond to incidents (impacts) when all else fails.

A word about Hackers…

1. They seldom care about collateral damage.
2. They often exploit the weakest link(s).
3. They have the element of surprise.

IBM's Approach

Focused on security essentials, informed by the IBM Security Framework

1. Build a risk-aware culture and management system

2. Manage security incidents with greater intelligence

3. Defend the mobile and social workplace

4. Security-rich services, by design

5. Automate security "hygiene"

6. Control network access and help assure resilience

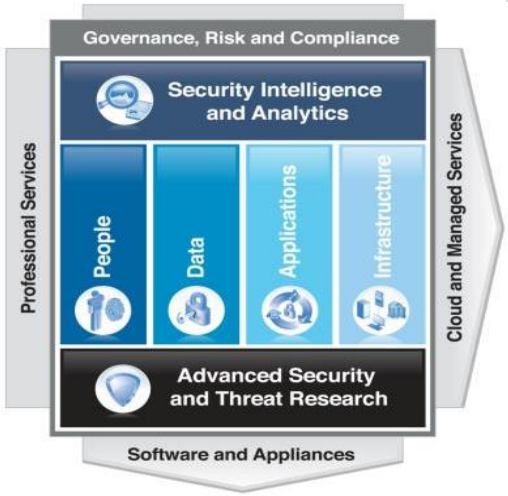
7. Address new complexity of cloud and virtualization

8. Manage third-party security compliance

9. Better secure data and protect privacy

10. Manage the identity lifecycle

IBM Security Framework



Financial Executives Cyber Security & Business Continuity Study Paper

April 2014, CFERF Study Key Points

1. Study produced from Online survey of senior financial executives across Canada in Nov-Dec, 2013
2. CFOs hold direct responsibility for IT at many organizations.
3. According to 68% of respondents, the CFO signs off and approves IT security spending, eclipsed only by the president and CEO
4. To improve security, participants observed that it was necessary to obtain buy-in by the rest of the C-Suite, including the CEO, board.
5. Study includes metrics, responsibilities, CFO perceptions, Executive recommendations. Get the study today !