ADVANCED PERSISTENT THREAT

Next Generation of Cyber Attacks

Leonard Ong, CPP
Werner Preining, CPP

ASIS International Asia Pacific Conference

4-5 December 2013

Agenda

- Key Trends
- Advanced Persistent Threat (APT) defined
- APT Risk Management
- Q & A

Key Trends

1. Data is the new oil
   - Up to 2003: Five Exabytes of information generated by civilization
   - YR 2012: Two Exabytes of new information **Every Day**
   - YR 2013: Five Exabytes of new information **Every 10 mins**

2. Information leaks all the time

1. Stricter regulations and legal implications

2. Best practices as basic business expectation

Source: “How much information?” Peter Lyman, Hal Varian |The Case against digital sprawl, IBM | ISF Threat Horizon 2015

Key Trends

- Data Set:
- 47,000 incidents
- 621 confirmed data breaches
- 2,500 data breaches in total
- 1.1 billion compromised records

- 19 Global organizations from
- Australia, US, Denmark, Dutch, Spain, Ireland, Malaysia.

- 9 Years running.

Key Trends

verizon 2013 DATA BREACH INVESTIGATIONS REPORT

Who are the victims?

- **37%** of breaches affected financial organizations (+)
- **24%** of breaches occurred in retail environments and restaurants (-)
- **20%** of network intrusions involved manufacturing, transportation, and utilities (+)
- **20%** of network intrusions hit information and professional services firms (+)
- **38%** of breaches impacted larger organizations (+)
-  **27** different countries are represented

Who's perpetrating breaches?

- **92%** perpetrated by outsiders
- **14%** committed by insiders (+)
- **1%** implicated business partners
- **7%** involved multiple parties
- **19%** attributed to state-affiliated actors (+)

Key Trends

verizon 2013 DATA BREACH INVESTIGATIONS REPORT

What commonalities exist?

- 75% driven by financial motives (-)
- 71% targeted user devices (+)
- 54% compromised servers (-)
- 75% are considered opportunistic attacks (-)
- 78% of initial intrusions rated as low difficulty
- 69% discovered by external parties
- 66% took months or more to discover (+)

How do breaches occur?

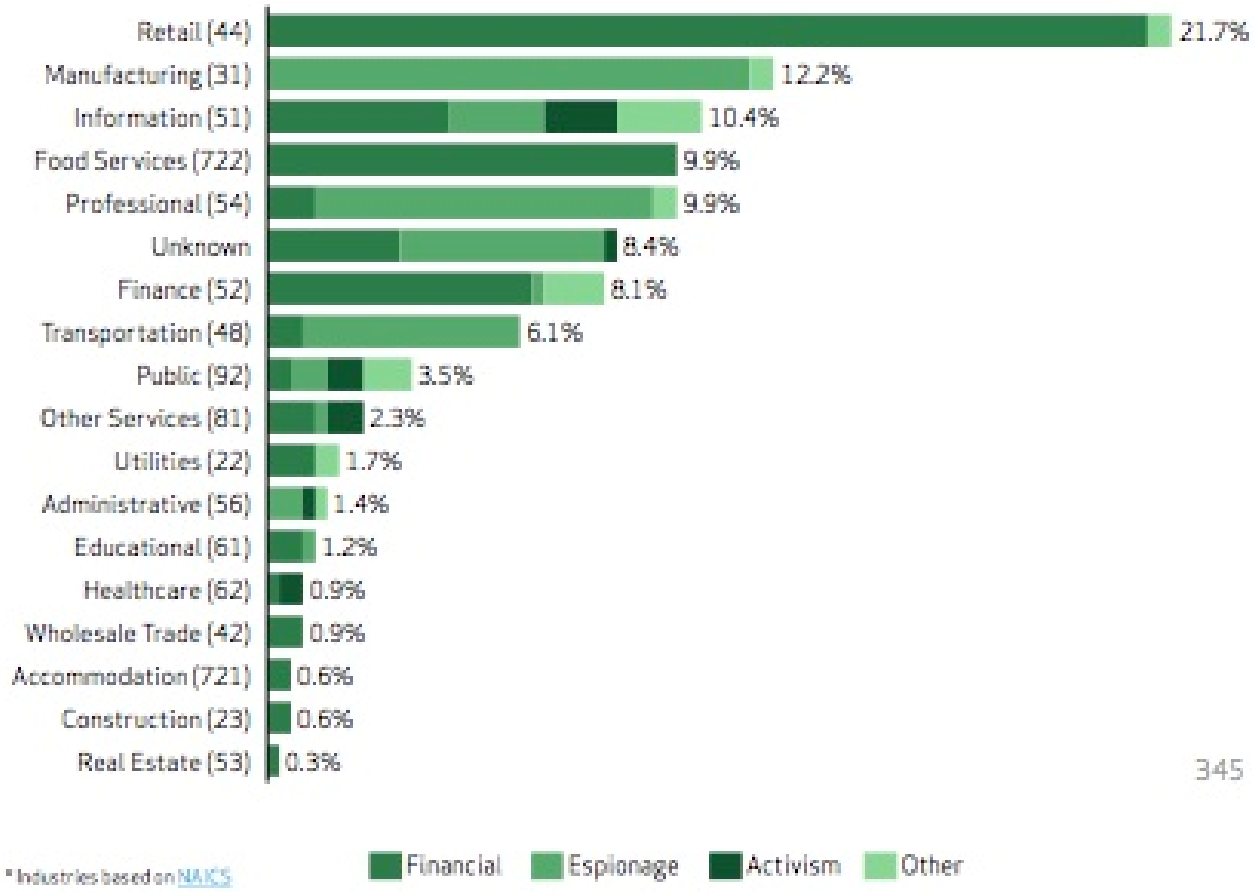
- 52% used some form of hacking (-)
- 76% of network intrusions exploited weak or stolen credentials (-)
- 40% incorporated malware (-)
- 35% involved physical attacks (+)
- 29% leveraged social tactics (+)
- 13% resulted from privilege misuse and abuse

Key Trends

verizon

2013 Data Breach Investigation Report

Figure 3: Victim industry (filtered for network intrusions)*



* Industries based on NAICS

2015 Threat Horizon

Reputation is a new target for Cyber attacks	Insiders being enablers. Hacktivists create fear, uncertainty and doubts.
Criminals value your information	Crime as a Service v2.0.
Cyber Risk is challenging to understand and address	Top Management support, Outsourcing woes, Competent resources
The Challenging face of technology does not help	Bring your own Cloud/Device/Experience
The role of Government must not be misunderstood	The Government and Regulators won’t do it for you

Top Threats for Multinational Companies

External Threats

- Distributed Denial of Service
- Advanced Persistent Threats
- Hacktivism

Internal Threats

- Ineffective controls
- New technologies
- Budget constraint
- Outsourcing

Regulatory Threats

- Diverse regulatory landscape
- New requirements with limited time to comply
- Lack of universal regulatory taxonomy

Advanced Threats

9/11

Perpetrators identified

StuxNet

Non-Attributable

Key Trends

Just **46.6%** of respondents believed that APTs were a unique threat.

And more than half **(53.4%)** believe this advanced set of threats is no different to what they've been dealing with in the past.

WHAT DOES THIS MEAN?

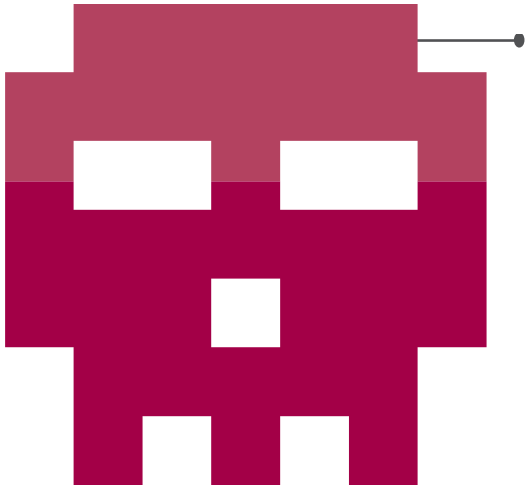
Source: ISACA, APT Awareness Survey Result

Key Trends

Suffering with an APT

Although just **21.6%** of respondents reported having been victims of an APT attack

63% – three times that amount – believe it's only a matter of time before their business is targeted.



63%

BELIEVE IT'S ONLY A MATTER OF TIME BEFORE THEIR BUSINESS IS TARGETED.

Source: ISACA, APT Awareness Survey Result

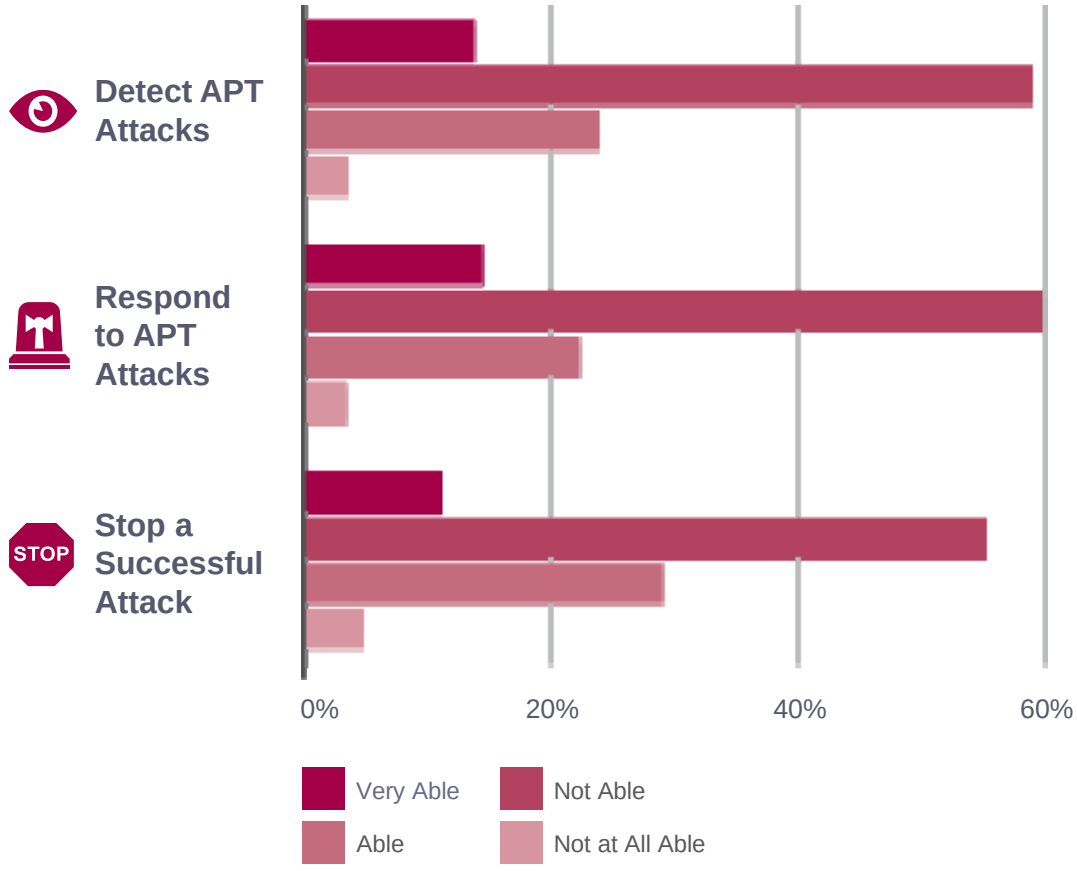
Key Trends

The majority of survey takers – up to **60%** – believed that they have the ability to ID, respond to and stop a successful APT attack.

31.1% said they have incident management plans in place to fight an APT.

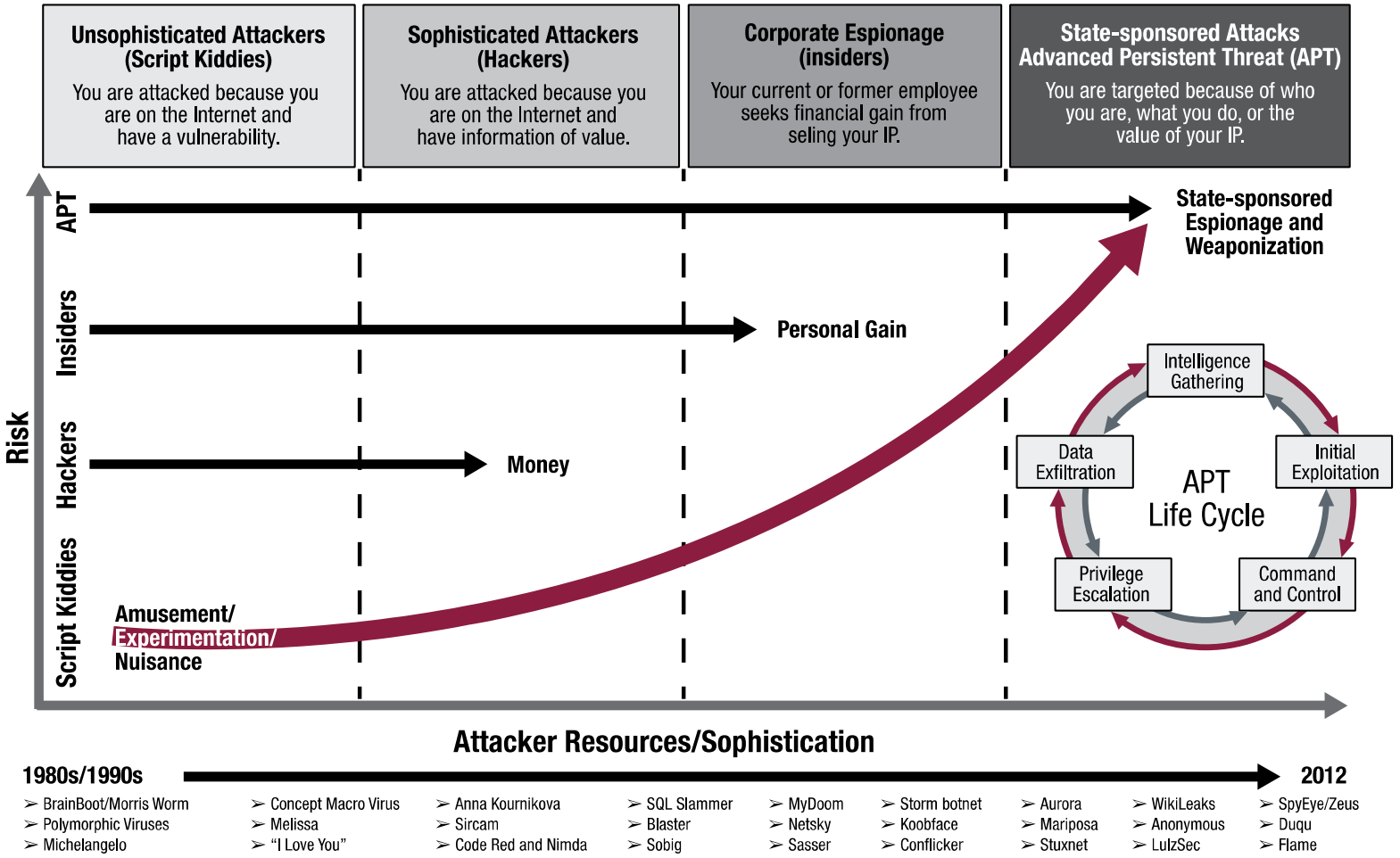
49.5% are prepared, but without a concrete solution.

How able is your enterprise to deal with an APT attack?



Source: ISACA, APT Awareness Survey Result

Evolution of Threat Landscape



Source: ISACA, Responding to Targetted CyberAttacks

Adaptive Attack Vectors

Multi-Factor Authentication

- Break into token vendor and steal keys

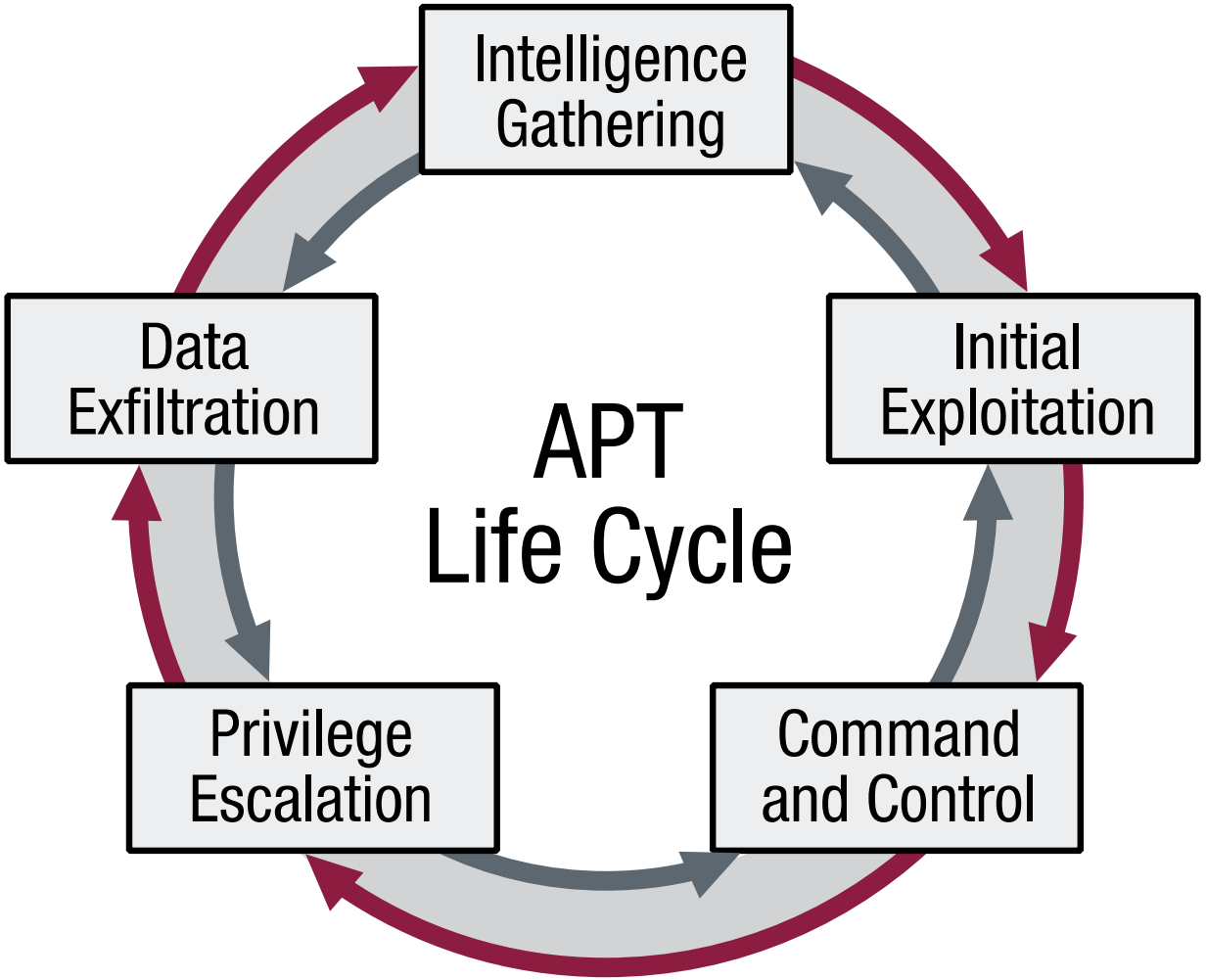
Application Digital Signature

- Use legitimate code signing infrastructure of popular applications

Application Whitelisting

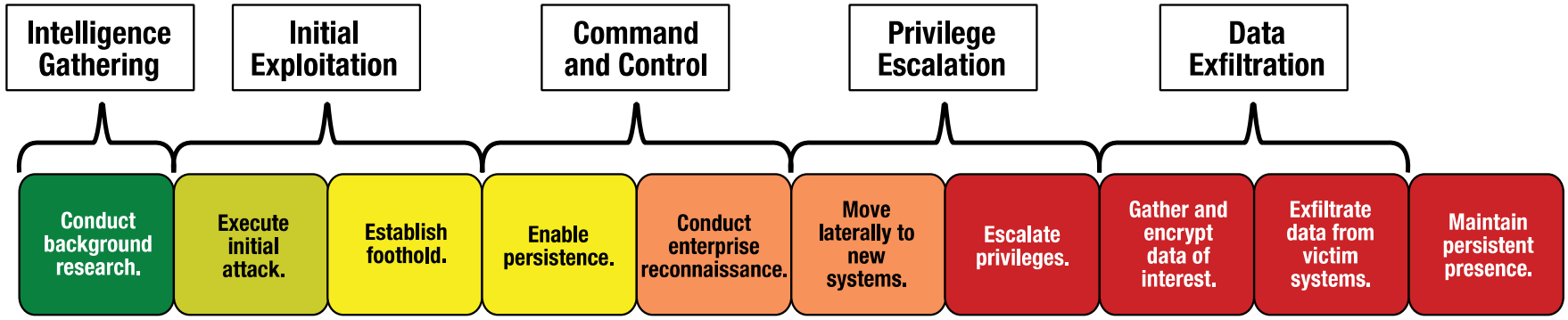
- Break into code-signing infrastructure and sign malware for whitelisting

APT Life Cycle



Source: ISACA, Responding to Targetted CyberAttacks

APT Life Cycle



Source: ISACA, Responding to Targetted CyberAttacks

Modus Operandi

Network Perimeter Security
- Encryption

Application aware gateways
- *Hiding in plain sight.* Common services

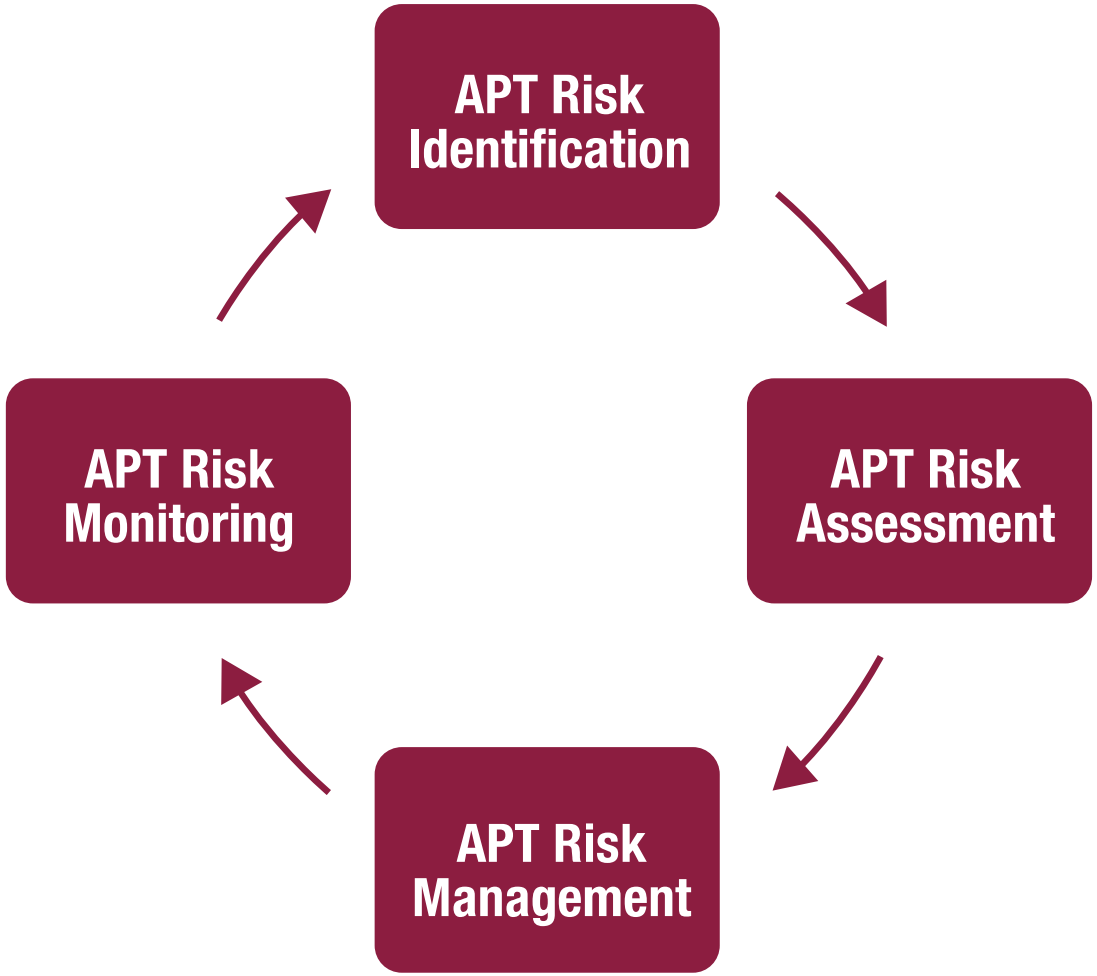
End-point Security
- Fresh malware
- Tested in AVs

Content filtering
- Link to malware

URL Filtering
- Compromise good known websites

Regular assessment
- Zero-day attacks
- Indirect action

APT Risk Management Cycle



Source: ISACA, APT: How to manage risk to your business

APT Controls Review

QUESTIONS & COMMENTS