www.pwc.de

Assuming a state of compromise.

A best practice approach for SMEs on incident response management.
May 2014

pwc

Agenda

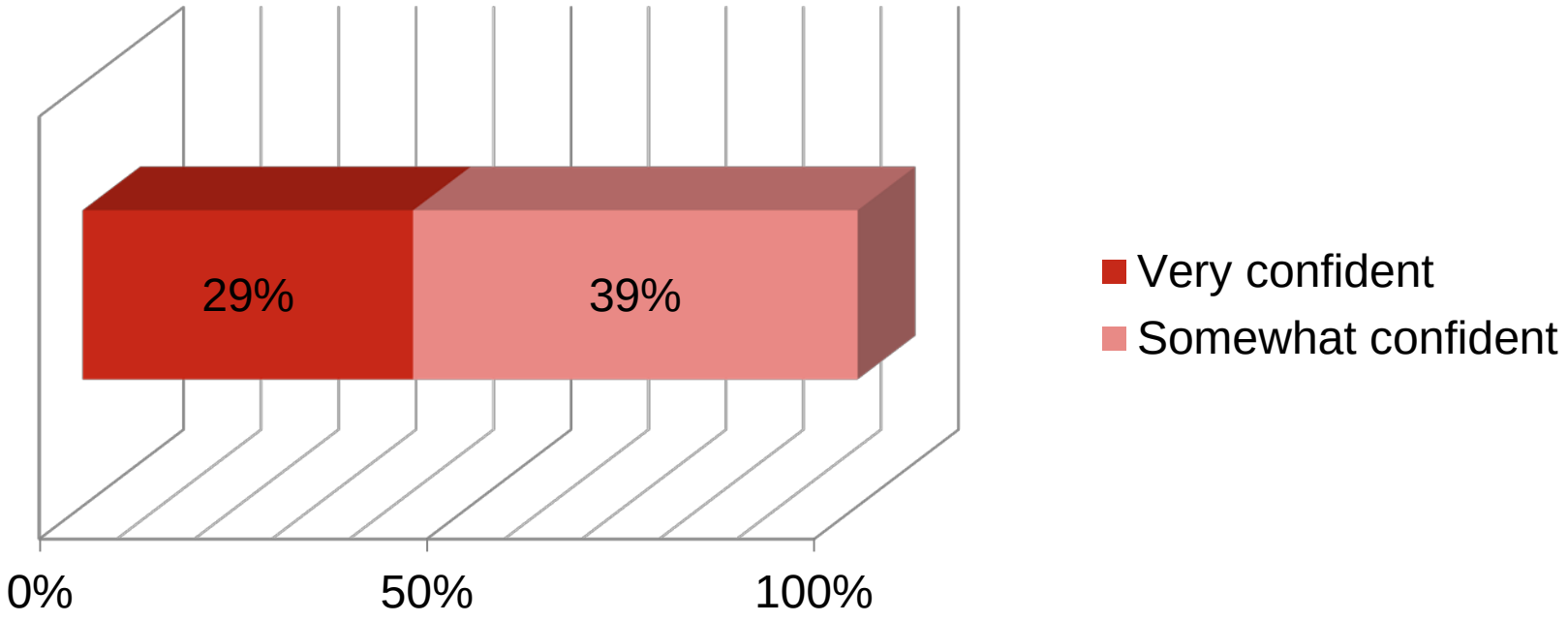
- Motivation
- Characterization of Risks
- Problems and Challenges of SMEs
- A New Cyber Security Philosophy
- Conclusion

Motivation

1

Information security behaviors

To be effective, security must be integral to the way people think and work, not just another item to be checked off a list.



Source: The Global State of Information Security® Survey Question 35 - "How confident are you that your organization has instilled effective information security behaviors into the organizational culture?" (Not all factors shown. Totals do not add up to 100%.)

What makes SMEs prone to Cyber-Attacks?

IT infrastructure is growing without concept

Lack of monetary budget for IT infrastructure and trainings

SMEs rarely involved in IT security initiatives

Internal monitoring is lacking maturity

No specified responsibilities like CISO

No own IT department

Assuming a state of compromise.

Characterization of Risks

2

The Cyber Threat Landscape

Cybercrime is committed by a multitude of offenders with diverse motives.

Targets

- Trade secrets
- Sensitive business information
- Emerging technologies
- Critical infrastructure

- Financial / payment systems
- Personally Identifiable Information
- Payment Card Information
- Protected Health Information

- Critical infrastructure
- Operational technologies
- Highly visible venues

- Corporate secrets
- Sensitive business information
- Information related to key executives, employees, customers & business partners

Assuming a state of compromise.

Problems and Challenges for SMEs

3

Recognizing Breach Indicators

Unauthorized web pages created on an Internet-facing web server

Data transmitting outbound over unlikely protocols

Large compressed files being transmitted outbound

Unusual connections between a user systems using native operating system networking features

Log entries on domain controllers capturing the execution of unauthorized programs

Assuming a state of compromise.

Common mistakes observed…

Assigning the organization's IT operations department to investigate the incident

Incident response becomes a technically centric endeavor

Investigative actions are not forensic

Collaboration and sharing information between companies is extremely important in cybersecurity but requires trust, which is still not available

Why are especially SMEs susceptible to cyber threats?

- Generic user accounts are used for administrative tasks
- No segregation of rights is practiced because of convenience reasons
- The aim of an IT department respectively the management is just the faultless operation of the IT infrastructure
- Technological sentinels remain critical assets for managing cyber risk.
- A cybercrime investigators mindset to daily cyber security operations is a much needed capability

A New Cyber Security Philosophy

4

Assuming a state of compromise

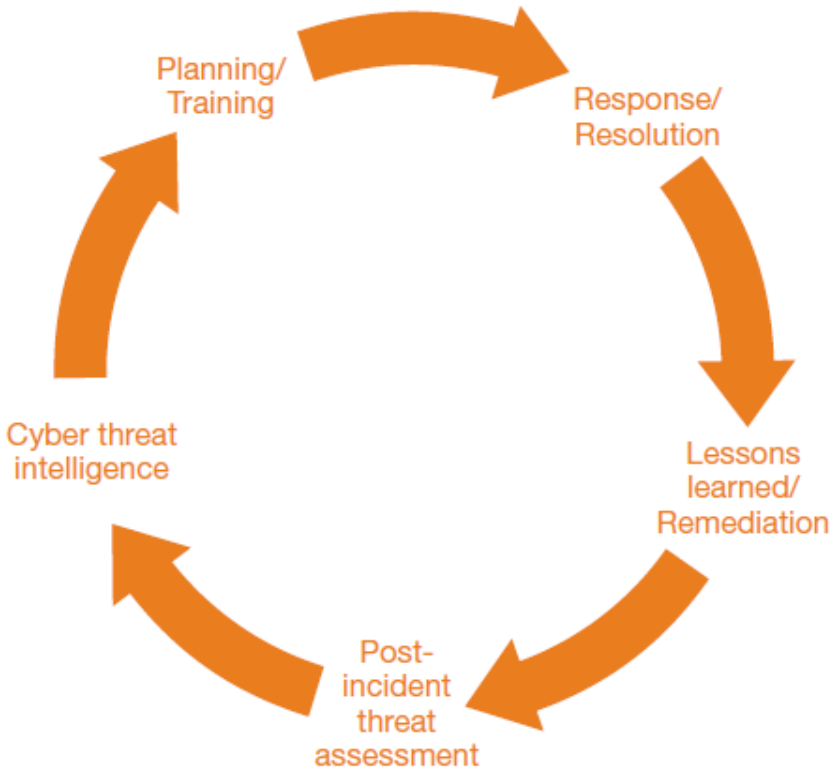
Our approach assumes:

- an active and perpetual state of compromise,
- seizing all opportunities to gather cyber threat intelligence,
- transformation of the IT environment into a treasure trove of digital evidence,
- assessment of the state of security of its interconnected vendors,
- recognition of the authorized insider as a cyber threat,
- a forensic incident response capability.

The need for change

The future of cyber security is going to require an evolved philosophy that assumes a never-ending state of compromise.

A New Cyber Security Philosophy



Cyber Incident Management Lifecycle

Emerging Cyber Security Methods

Historical cyber security

Use signature-based monitoring technology such as firewalls, intrusion detection/prevention systems, proxy servers, and anti-virus (A/V) systems to detect suspicious activity.

- Reduce the number of human staff.
- Focus detection on critical data stores and network perimeter.
- Minimize logging on user systems.
- Let A/V software secure user systems.
- Let IT configure monitoring technology.
- Let IT investigate suspicious events.
- Treat security assessments as a series of one-time events, or 'checking a box.'

Emerging cyber security

- Enhance signature-based technologies with custom rules and alerts informed by a cybercrime mindset.
- Collect and maintain all logs from monitoring technology and systems.
- Focus detection on all systems, not just on critical data stores and external-facing computers.
- Increase operating system logging on all systems.
- Have a systematic method to collect and analyze live memory on systems.
- Collect and maintain all network traffic.
- Minimize Internet-access points.
- Baseline network traffic.
- Use a limited set of system configurations and baseline them.
- Analyze all phishing emails.
- Analyze all malware.
- Have a cyber incident response framework that relies upon experienced cybercrime and cyber forensics resources.
- Have an all source cyber intelligence program.
- Have an ongoing security assessment program and immediately address areas of risk.
- Have a program to assess and identify high risk insiders.

Conclusion

5

Conclusion

- Cybercrime and those who commit it are always evolving, focused on accessing sensitive information and maintaining persistent remote access for as long as possible.
- In our approach we showed methods and tools for SMEs, to get knowledge about their state of compromise.
- As well, we want to highlight that this paper is not intended to be the silver bullet for fighting cybercrime.
- The future of cyber security is going to require an evolved philosophy that assumes a never-ending state of compromise.

Thank you.