Incident Response Pre-Planning

1/14/2020

Speaker Introduction

Scott E. Gicking

Director, PwC Advisory Cyber & Privacy

Mobile (818)319-2361 | Scott.e.gicking@pwc.com

Scott is a Strategy and Transformation Director based in San Diego. With over 20 years of cybersecurity experience, Scott specializes in reviewing cybersecurity programs to collaborate on transformation strategies for more effective programs. He conducts comprehensive cybersecurity assessments, gap analysis and road mapping across various industries. Scott also acts as a CISO Advisor for companies in transition of cybersecurity leadership working close with the C-Level executives on building up their strategies and future capabilities, maintaining operational capability and identifying and on-boarding new leadership for the program.

Scott is a former CSO/CISO for a billion-dollar digital media company. He established a comprehensive global security program, built a team, designed departments, roles and responsibilities, developed strategic planning and provided regular updates on mitigating strategies to executive levels of the company.

Prior to the CISO role, Scott spent over 25 years with the FBI where he gained a deep understanding of the threat landscape and the strategic options to mitigate risk. Scott maintains his accreditation as a Certified Information Systems Security Professional (CISSP).

HBO Hacked!!

http://www.youtube.com/watch?v=j38seJ2es0A

HBO Ransom Note

Dear Richard Plepler;

I am Mr. Smith and I have the honor to inform you, on behalf of my colleagues, that we successfully breached into your huge network.

We are glad to say that in a complicated cyber operation, infiltration to your network accomplished and we obtained most valuable information. (1.5 Terabyte)

We confess that HBO was one of our difficult targets to deal with but we succeeded. (It took about 6 months).

By penetrating your Internal Network and other related platforms, we obtained your highly confidential Documents, IT related data, Scripts and etc. these data dump, as you will see, contains HBO's Various Contracts, Mutual Agreements, Human resources, internal structure, International affiliates, Business strategies, international Marketing, IT infrastructures, producing films & Series (with very detail info!), budget detail for major operations, how you sell and how much!, various strategic insights in every aspects, confidential research, internal letters & Tax Evading Proofs! & Nielsen's Dirty Job! & etc.

HBO Ransom Note

Leakage will be your worst nightmare; your competitors will know about your current & future strategies, your inner circle inside HBO & senior staff will be thrown into chaos, your viewers specially fans became very upset and they blame you rather than us!, downfall in stocks will be predictable and so on. As you are in the business from decades, you yourselves will be full aware of catastrophic consequences .... So make a wise decision!

There are 2 mottos. Which one is remembered?

Winter is Coming --- HBO is Falling

OR

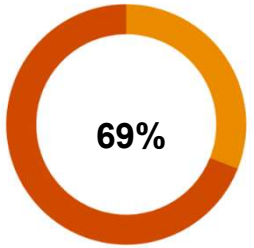
Winter is Coming --- HBO is standing & EverLasting !

HBO Ransom Note

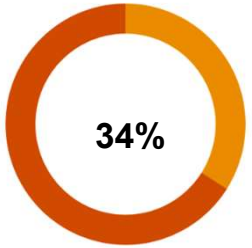
Cyber threats 2019 – Year in retrospect

"Cyber resilience includes the agility of both defense and recovery capabilities. Resilient systems help companies to sustain operations when possible amid cyberattacks and to rapidly recover in the event of disruption. Only about half of medium and large businesses in key sectors say they are building resilience to cyberattacks and other disruptive events to a large extent. And fewer than half of them say they are very comfortable their company has adequately tested its resistance to cyberattacks.

PwC 2019 Digital Trust Insights Survey

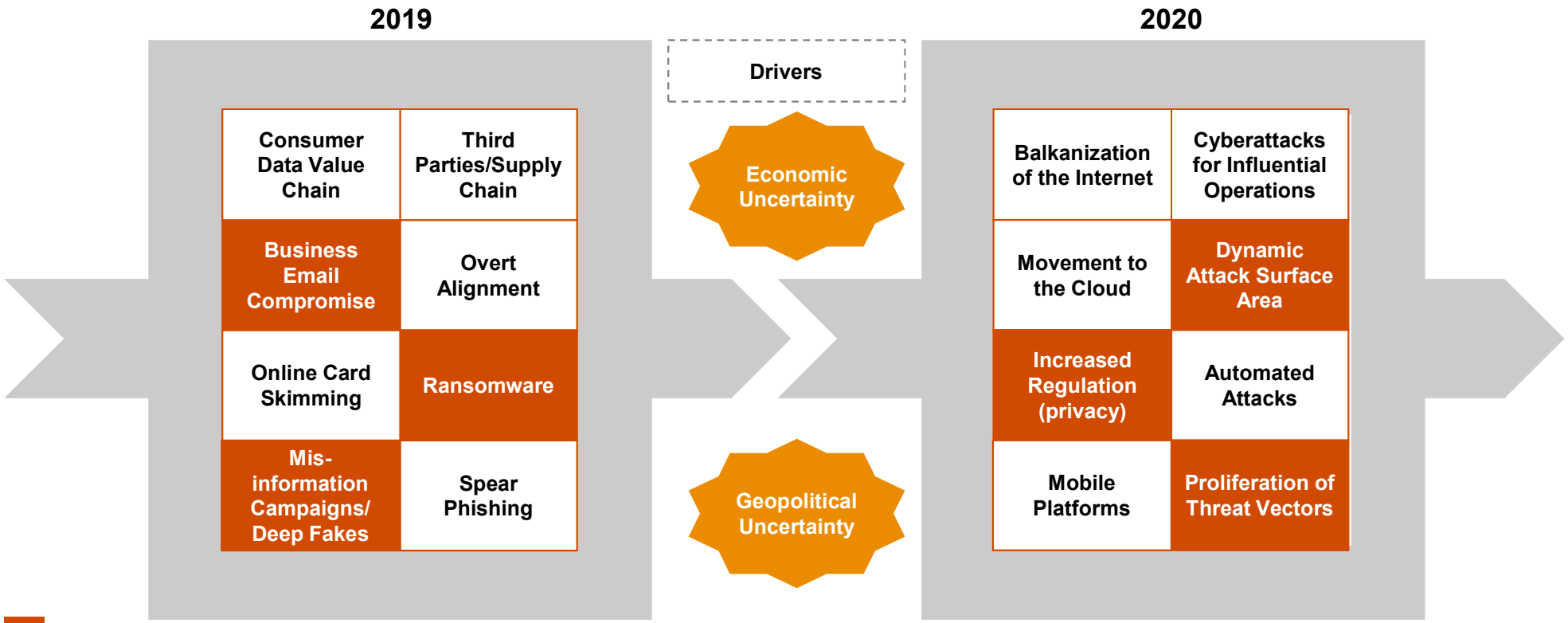


Of the organizations who suffered a cyber-attack, more than two-third felt that they did not have adequate capabilities to respond to an incident.



Only 34% of business leaders expressed that they are very comfortable with how adequately their company has tested its cyber-incident response plan.

Trends in cybersecurity incidents



Key points

Lessons from major cyber breaches

1

Weakest link

Attackers are continuing to take advantage of organizations yet to master the “hard basics” of cyber security.

2

Out of control

Organizations cannot always control when they will be breached, but they can control how they respond.

3

Increasingly complex

Time pressures for organizations to effectively respond to incidents are increasing while incidents become more complex.

4

Focus on coordination

Management and coordination of major incidents is a more significant challenge to organizations than technical analysis.

5

Outsourcing

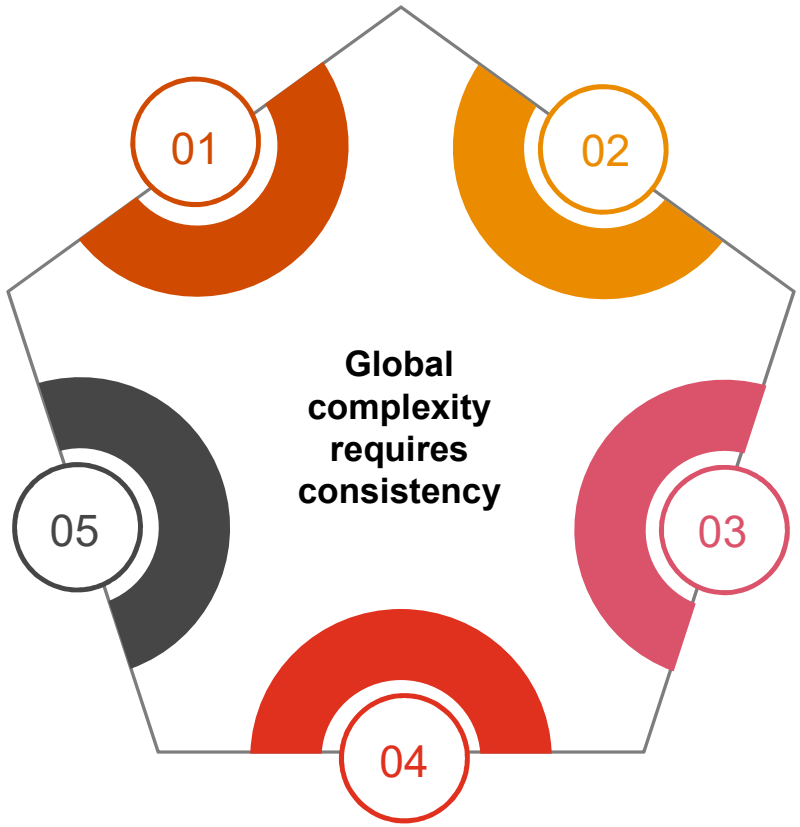
Outsourced service providers can be the key enabler, or the key barrier, to an effective incident response (and in some cases even the cause of the incident).

6

Investment

Organizations are increasing their investment budget to enhance detection and response capabilities as threats evolve.

Why incident response matters to the executive committee



01 Prevalence
The increase in the amount of threat actor groups and IT surface area has resulted in the prevalence of multi-faceted cyberattacks.

02 Efficiency & coordination
Incident Response is not simply a technical issue. Executives must coordinate across business functions and establish metrics to drive efficiency and coordination.

03 Awareness
Many executives are unfamiliar with the incident response process and the components involved across the incident response lifecycle.

04 Downstream implications
Cyberattacks may begin as a technical issue, but can have downstream implications - financial, reputational, customer-centric, regulatory, and operational.

05 Visibility and accountability
Understanding executive roles and responsibilities to drive oversight will increase visibility and accountability across the incident response lifecycle.

Best practices for incident response

Formalize your incident response plans

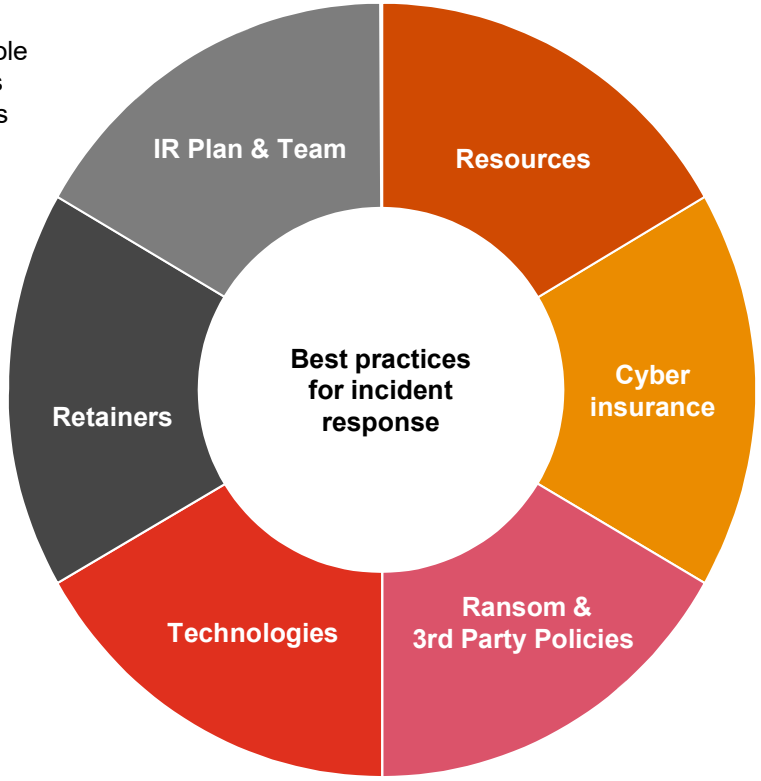
- Name and communicate X-functional teams, role and responsibilities, RACIs and outside parties
- Establish escalation criteria & severity matrices
- Regularly practice the plan through tabletop exercises and scenarios

Establish retainers

- Establish external incident response retainers with reputable firms (law firms, crisis communications, PR, forensic)
- Involve your retainer partners outside incidents
- Understand the terms, conditions and activation pathways of the retainer agreement

Ensure coverage and visibility

- Ensure enterprise coverage and endpoint visibility through cybersecurity tools
- Ensure business processes and policies span across the enterprise



Commit resources and support

- Commit and train incident response resources
- Fund training, certifications, conferences, simulations
- Support technologies, equipment, network visibility investments
- Recognize job demands

Incorporate cyber insurance

- Establish a cyber insurance provider
- Understand services provided by the cyber insurance firm including breach costs, customer costs, business interruption costs, and remediation costs

Determine corporate perspective on ransom payments & interactions with 3rd parties

- Corporate policy on ransom payments; Consider establishing a Bitcoin wallet in advance
- Media & third party communications policy (threat researchers, bug bounty, reporters)

Looking ahead

Incident response challenges in 2020

Competing for talent

Moving to the cloud

Insider threats

Cyber investment strategy

Increased regulation

Key takeaways

Establish a core team

- Establish key stakeholders to formulate a Core Team
- Establish roles and responsibilities for incident response

Understand threat vectors

- Familiarize with common threat vectors in the industry
- Socialize threat vectors across core team stakeholders

Determine risk appetite

- Understand pertinent cybersecurity risks across functional areas
- Determine threshold of cybersecurity risk within the organization

Test response capabilities

- Conduct tabletop simulation exercises with relevant scenarios
- Track and gauge incident response capabilities with data driven KPIs

Questions?

Thank you

Scott E. Gicking
Director, PwC Advisory Cyber & Privacy
Mobile (818)319-2361 | Scott.e.gicking@pwc.com

pwc.com