THE one BRIEF
AON EXPLORES THE WORLD'S MOST PRESSING BUSINESS ISSUES

RISK & INNOVATION

Infographic: Are You Prepared For A Cyber Attack?

April 14th, 2016

OVERVIEW

As more people and devices connect, the risk and impact of data breaches from malicious cyber attack, system failures and human error will only continue to increase.

Recent high profile cyber breaches have revealed how complacency on the part of senior leadership can lead to massive damage to an organization's bottom line and reputation. From scenario planning to cyber risk assessments, there are growing measures organizations can take to understand vulnerabilities and prepare for this growing threat.

Cyber attacks have the potential to cause massive business disruption, wreak tangible property damage, disrupt supply chains and even lead to injury or death. By adopting individual and organizational measures combined with a thorough risk management framework, companies can begin to reduce the cyber threat.

Explore below for key facts and figures that all organizations need to know in this age of growing cyber risk – and some practical steps you can take to help address the challenge.

IN DEPTH

THE one BRIEF
theonebrief.com

CYBER ATTACKS
ARE YOU PREPARED?

CYBER IN CONTEXT

FUTURE OF CYBER

50 BILLION DEVICES

WILL BE CONNECTED TO THE INTERNET BY 2020.[1]

THAT'S 8 DEVICES FOR EVERY PERSON GLOBALLY.

MORE DEVICES = GREATER RISK

THIS CREATES MORE CHANCES FOR MALICIOUS ATTACKS, HUMAN ERRORS AND SYSTEM FAILURES.

SOURCE OF THREATS

Types of breaches[2]

Days to detect breaches[3]

TOP 5 CONCERNS[4]

1. **Business interruption** (during breach)
2. **Business interruption** (after breach)
3. **3rd party liabilities**
4. **Breach due to 3rd party systems**
5. **1st party breach cost**

Sources

[1] Ponemon Institute, 2015 Global Cyber Impact Report (sponsored by Aon).
[2] Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis.
[3] Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis.
[4] Ponemon Institute, 2015 Global Cyber Impact Report (sponsored by Aon).

THE one BRIEF

AON Empower Results®

THE one BRIEF
theonebrief.com

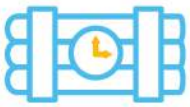
CYBER ATTACKS
ARE YOU PREPARED?

COST OF CYBER

FINANCIAL COST OF ATTACKS

$300 BILLION

COST TO U.S. COMPANIES DUE TO CYBER ESPIONAGE AND I.P. THEFT BY FOREIGN COUNTRIES.[1]



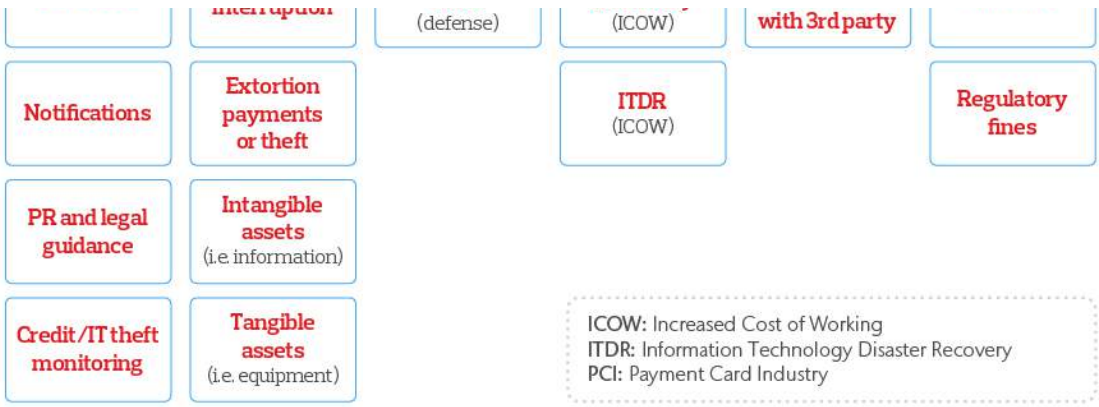
$617 MILLION

AVERAGE PROBABLE MAXIMUM LOSS FROM THEFT AND/OR DESTRUCTION OF INFORMATION ASSETS.[2]

34%

OF THIS LOSS STEMS FROM BUSINESS DISRUPTION TO INFORMATION ASSETS.[3]

Breakdown of attack costs



Cyber attacks can have real, financial consequences – why do so few large organizations budget for cyber cover?

The lack of budget for cyber-related expenses could indicate certain levels of complacency on the part of senior leadership.

The massive, well-publicized attacks against large companies over the past two years show that this complacency could lead to tremendous damage to a company's bottom line.

Sources

[1] U.S. Commission on the Theft of American Intellectual Property, The IP Commission Report, 2013.
[2] Ponemon Institute, 2015 Global Cyber Impact Report (sponsored by Aon).
[3] Ponemon Institute, 2015 Global Cyber Impact Report (sponsored by Aon).

THE one BRIEF

AON
Empower Results®

THE one BRIEF
theonebrief.com

CYBER ATTACKS
ARE YOU PREPARED?

APPROACHES TO CYBER

WHO BUYS CYBER INSURANCE?

19%
of companies currently have cyber insurance coverage, with an average limit of $13 million.[1]

54%
of companies have no plans to buy cyber insurance, despite an expected increased exposure to cyber risks.[2]

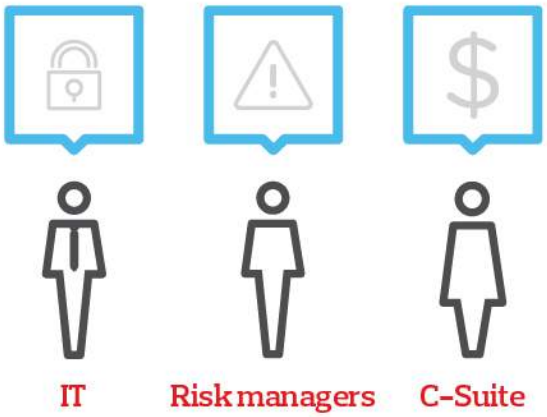
75%
of data handlers (health care, retail, and financial service sectors) have purchased cyber insurance.[3]

Data handlers' high rate of cyber insurance uptake could be a response to the sector's dramatic increase in the scale and severity of cyber attacks.

#1 reason
heavy industry companies (construction, engineering, manufacturing, and forestry products) purchase cyber insurance is for due diligence and comfort of board.[4]

This concern for due diligence is possibly because of confusion over which insurance policies would cover physical damage caused by cyber attacks.

STAKEHOLDER DIFFERENCES



Different stakeholders have varying perspectives about cyber risks.

IT: Focused on the technical issues facing the business.

Risk Managers: Trying to assign appropriate risk owners and build enterprise strategies.

C-Suite: Know it is a strategic issue but struggle to define balance sheet impact.

Sources

[1] Ponemon Institute, 2015 Global Cyber Impact Report (sponsored by Aon).
[2] Ponemon Institute, 2015 Global Cyber Impact Report (sponsored by Aon).
[3] Aon, Cyber – The Fast Moving Target Report, 2015.
[4] Aon, Cyber – The Fast Moving Target Report, 2015.

THE one BRIEF

AON
Empower Results®

THE one BRIEF
theonebrief.com

CYBER ATTACKS
ARE YOU PREPARED?

EFFECTIVE CYBER RESPONSE

RISK MANAGEMENT FRAMEWORK

1 Preparation

2 Practice

3 Execution

The risk from cyber attacks can't be completely eliminated, but it can be greatly diminished through proactive measures and implementing a thorough risk management framework.

CYBER RISK ASSESSMENT STEPS

1

Scenario Analysis
Benchmark the existing cyber risk profile and work with business stakeholders to prioritize cyber risk scenarios.

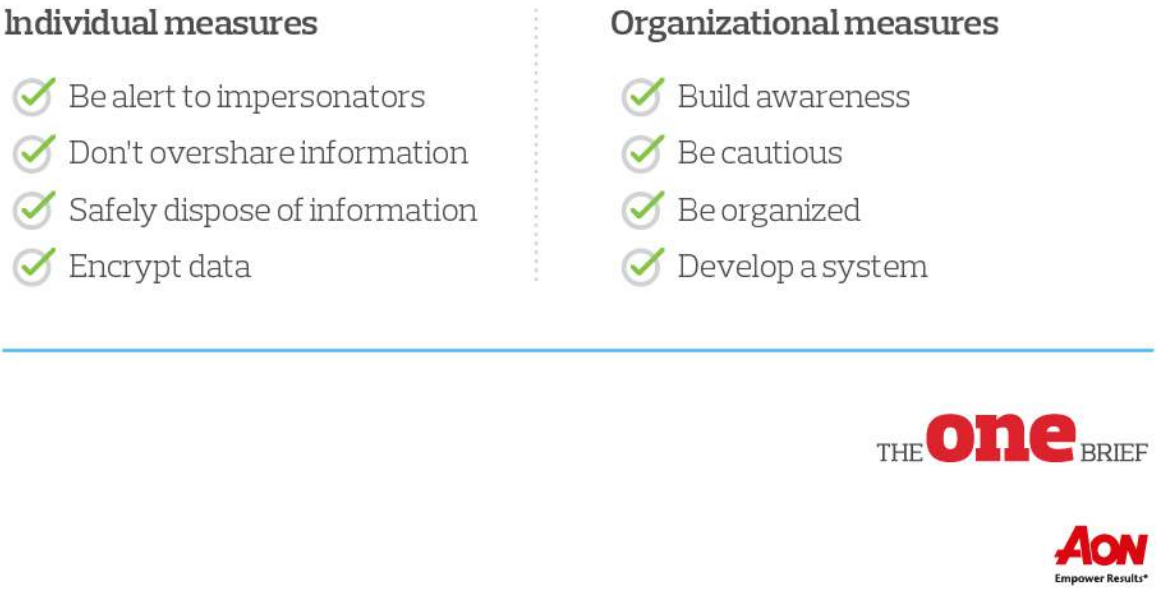
2

Financial Modelling
Leverage financial simulation tools to quantify first and third party costs of select cyber scenarios. Consider potential business interruption scenarios using forensic accounting.

3

Insurability Risk Review
Test the adequacy of limits against the assessed cyber risk as well as review the optimization of the proposed insurance program.

CYBER PROTECTION CHECKLIST



TALKING POINTS

"As the speed of innovation and digital transformation outpaces risk management and insurance strategies, companies need to break down silos between functional teams to keep up with their cyber threat. Cyber has created a divide across organisations with perceptions of the magnitude of the cyber threat varying between risk managers, IT teams, and the Board of Directors." – Adam Peckman, Global Practice Leader, Cyber Risk Consulting

"Conducting a cyber risk assessment is a useful tool for improving risk understanding and maturity as well as helping organizations better prepare for potential business interruption during or after a breach... [helping] translate cyber exposures into financial impact." – Kevin Kalinich, Global Practice Leader, Cyber / Network Risk

"Cyber is a relatively new area of risk that lacks concrete solutions and industry standards. As such there is a disconnect within organizations as to how to best handle current and future challenges. As cyber breaches are felt on more balance sheets, we anticipate more members of the C-suite investing in and preparing for this significant and emerging threat." – John Bruno, Chief Information Officer, Aon

FURTHER READING

- Cyber Security Budgets Not Rising In Line With Threats, Say Security Pros – Computer Weekly, March 22, 2016
- Businesses Underestimating Cyber Security Risks – Australian Financial Review, February 2, 2016
- Huge Rise in Hack Attacks As Cyber-Criminals Target Small Businesses – The Guardian, February 8, 2016
- Cyber: The Fast-Moving Target – Aon report
- 2015 Global Cyber Impact Report – Ponemon Institute, sponsored by Aon
- Aon Cyber Diagnostic Tool – online cyber self-assessment