CYBER

Cyber Tabletop Exercise

K&L GATES

PRESENTED TO K&L GATES

FEBRUARY 8th 2018

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

CYBER TTX: INTRODUCTIONS

SPENCER LYNCH
Managing Director, Stroz Friedberg

+ 15+ years in cyber security and digital forensics
+ Head of Stroz Friedberg London office
+ Maintains an active case load of litigation and data breach investigations

ROGER FRANCIS
Vice President, Stroz Friedberg

+ 14+ years in cyber security consulting
+ Leads the EMEA Security Advisory practice
+ Focused on breach response and governance

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

Agenda

+ **Introductions**	-
+ **Cyber Tabletop Rules**	-
+ **ACME Corp. Background**	-
+ **Inject One: Preparedness**	20 Minutes
+ **Inject Two: Response**	20 Minutes
+ **Inject Three: Recovery**	20 Minutes
+ **Analysis & Conclusions**	10 Minutes
+ **Question & Answer**	20 Minutes

CYBER TTX: TABLETOP RULES

BE HONEST

+ The tabletop is a learning tool first and foremost, so play honestly.
+ The exercise works best if you try not to fight it.

ASK QUESTIONS

+ Do not hesitate to ask questions during the exercise.
+ If a technical term is unfamiliar, ask for clarification.

YOU ARE THE CISO

+ For this scenario you can assume that you collectively represent the Chief Information Security Officer (CISO).
+ Bring your own experiences to the discussions.

CYBER TTX: ACME CORP. BACKGROUND

INDUSTRY

+ A global online retailer that is headquartered in London.
+ Growth is derived from regular strategic acquisitions.

ARCHITECTURE

+ Majority of IT is outsourced through a range of 3rd party service providers.
+ Primary customer database containing PII is hosted in Amazon Web Services (AWS).

REGULATORY

+ Scenario takes place post May 2018, so GDPR is in play.
+ Processes PCI regulated credit card data.

MATURITY

+ Never knowingly breached, but recently a direct competitor went through the wash.
+ The organisation has a CISO, no DPO, but extremely limited internal forensic expertise.

CYBER TTX: INJECT ONE

PREPAREDENESS

It is a Thursday afternoon in August 2018, the week prior EMCA Corp. (a direct competitor) posted a £250M loss off the back of a cyber breach that was widely regarded as poorly handled. The company failed to notify the Information Commissioner's Office (ICO) in a timely manner, released a number of contradicting statements, and bundled customer communications.

You receive an email from the ACME Corp. board of directors, are asking what is being done to protect the company from an impending cyber catastrophe?

\+ What constitutes preparedness?

CYBER TTX: INJECT TWO

RESPONSE

The following Friday morning an Anti-Virus (AV) alert is triggered on one of the critical ACME Corp. domain controllers. The 3rd party Managed Security Service Provider (MSS) pass on the critical alert, noting that the malware appears to be a Remote Access Trojan (RAT) variant, and recommend further investigation.

After some basic triage of the respective system, a suspicious folder is discovered that contains a dump of all of the employees user credentials and a number of very large encrypted files.

\+ How do you respond?

CYBER TTX: INJECT THREE

RECOVERY

The subsequent IR investigation by Stroz Friedberg unearths an advanced cyber-attack against ACME Coro., most likely perpetrated by a financially motivated attacker outside of European jurisdiction.

The Incident Response (IR) report details the breach most likely originating from communications with a trusted 3rd party on February 8th, and culminated in the likely exfiltration of 500MB of potentially sensitive Personally Identifiable Information (PII) and Payment Card Industry (PCI) customer records.

The report concludes with a number of detailed cybersecurity recommendations for recovering and hardening the company environment against similar attacks in the future.

\+ What do you do next?

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

CYBER TTX: ANALYSIS & CONCLUSIONS

PREPAREDNESS

+ What are the organisational Prevent, Detect, and Respond cybersecurity capabilities?
+ Does the organisation have an effective and tested Incident Response Plan (IRP)?
+ Does the organisation have an Incident Response Retainer in place?

RESPONSE

+ What type of network and endpoint visibility doe the organisation have?
+ Who is responsible for what during a cyber breach (Inc. external parties)?
+ How can you make informed decisions during an cyber breach?

RECOVERY

+ How do you effectively contain and then recover from a cyber breach?
+ Who, what, when do you notify regulators?
+ How do you manage the reputational fallout from cyber breach?

STROZ FRIEDBERG: UPCOMING EVENTS

PROTECT WHAT'S YOURS

WEBINAR SERIES | Bi-monthly | 3rd TUESDAY | Begins: FEB

Education to help the organization build a shared culture of cyber resilience.

Upcoming webinar:

Enterprise Risk Management: Breaking Down Silos

February 20, 2018 | 11AM ET | 16:00 GMT

As the physical and cyber worlds collide, Chief Risk Officers take center stage to manage cyber as an enterprise risk issue.

TECH TALK

WEBINAR SERIES | Bi-monthly | 3rd TUESDAY | Begins: MARCH

Technical discussions on proactive security testing solutions to strengthen an organizations cyber defences.

Upcoming webinar:

Security in the Cloud: Do's and Don'ts

March 20, 2018 | 11AM ET | 16:00 GMT

Understand the most common security issues organizations need to be aware of and manage when building their cloud systems.

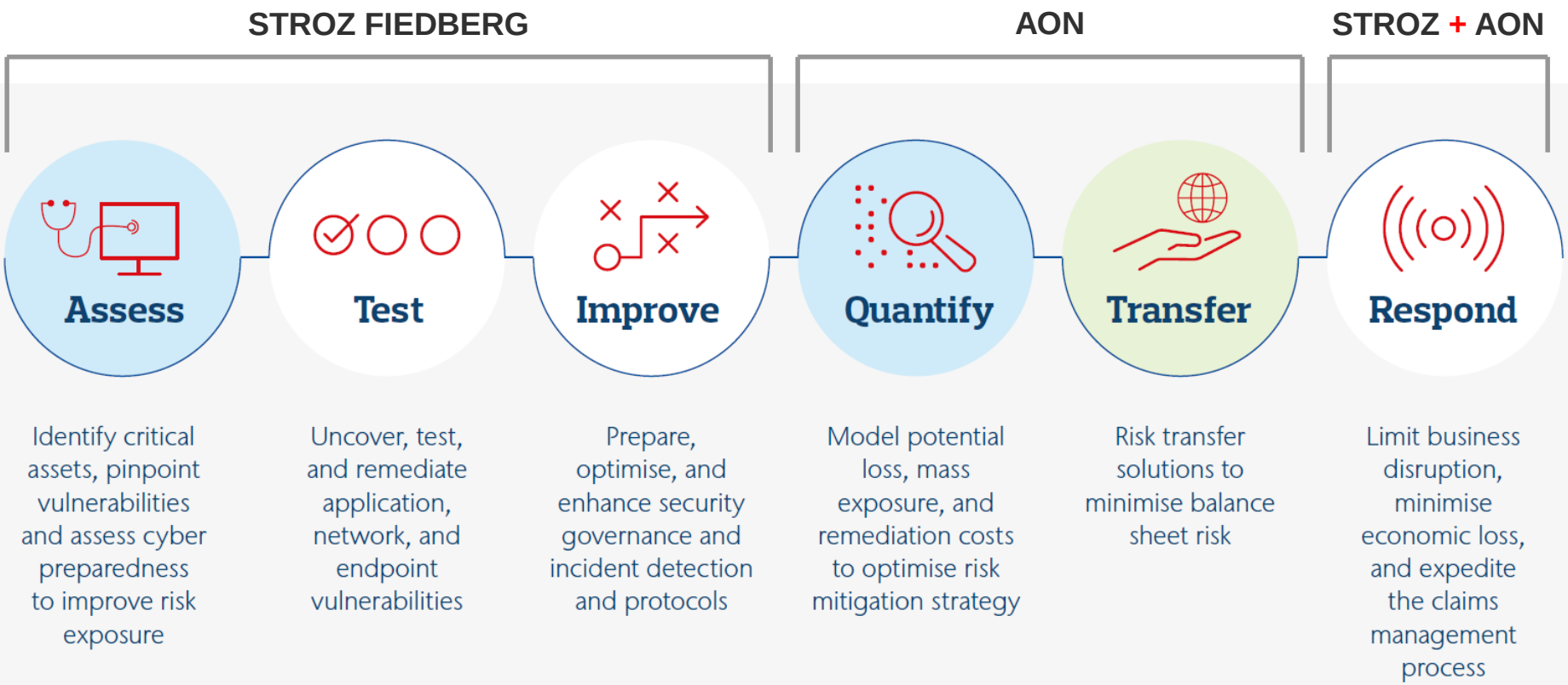
REGISTER AT STROZFRIEDBERG.COM

STROZ FRIEDBERG
an Aon company

AON
Empower Results®

CYBER TTX: STROZ FRIEDBERG

THE JOURNEY



STROZ FRIEDBERG
an Aon company

AON
Empower Results®

Contacts

STROZ FRIEDBERG
an Aon company

Mark Brannigan
Vice President
E mbrannigan@strozfriedberg.co.uk

Roger Francis
Vice President
Security Advisory Practice Lead
E rfrancis@strozfriedberg.co.uk

K&L GATES

Clarissa Coleman
Partner
E clarissa.coleman@klgates.com

Sarah Turpin
Partner
E sarah.turpin@klgates.com

STROZ FRIEDBERG
an Aon company

To learn more, visit www.strozfriedberg.com

Americas: +1 212.981.6540 | EMEA: +44 20.7061.2200 | Asia Pacific: +852 3187.8800

About Stroz Friedberg

Stroz Friedberg, an Aon company, is a specialized risk management firm built to help clients solve the complex challenges prevalent in today's digital, connected, and regulated business world. Our focus is on cybersecurity, with leading experts in digital forensics, incident response, and security science; investigation; eDiscovery; intellectual property; and due diligence. Stroz Friedberg works to maximize the health of an organization, ensuring its longevity, protection, and resilience. Founded in 2000 and acquired by Aon in 2016, Stroz Friedberg has thirteen offices across nine U.S. cities, London, Zurich, Dubai, and Hong Kong. Stroz Friedberg serves Fortune 100 companies, 80% of the AmLaw 100, and the Top 20 UK law firms. Learn more at https://www.strozfriedberg.com.

AON
Empower Results®