COVID-19 - Guidance for Businesses Navigating Regulatory, Operational and Cyber Threats

March 19, 2020
2:00 – 3:00 pm SGT
Host

Louisa Vogelenzang
Associate Managing Director
Identity Theft and Breach Notification
Kroll, a division of Duff & Phelps
louisa.vogelenzang@kroll.com

Speakers

Koh Sin Yee
Director
Compliance Regulatory Consulting
Duff & Phelps
sinyee.koh@duffandphelps.com

Simon Ashenden
Associate Managing Director
Security Risk Management
Kroll, a division of Duff & Phelps
simon.ashenden@kroll.com

David Klopp
Associate Managing Director
Cyber Risk
Kroll, a division of Duff & Phelps
simon.ashenden@kroll.com
Housekeeping

• Q&A will be held at the end of the presentation and questions can be asked throughout.

• Submit your questions through the Q&A widget which can be found at the bottom of your screen.

• The slides and webinar recording will be shared with you in approximately 3 working days after the webinar.
Disclaimer

• This presentation is made available by Duff & Phelps and Kroll for educational purpose only.

• Content is not to be used as legal opinion or as a substitute to qualified matter-specific legal advice within your jurisdiction.

• All endeavours have been made to ensure content’s accuracy as at the time of the webinar.
Today’s Agenda

• **COVID19**: Key points for financial services firms

• Crisis Management During Outbreak

• Unseen Risks and Threats

• Q&A
COVID19: Key Points for Financial Services Firms
Outline

• Does COVID-19 trigger any obligations for Financial Institutions in Singapore?

• What have we seen among our clients in terms of Business Continuity Management (BCM) compliance?

• How current events illustrate the importance of having a Business Continuity Plan

• Future developments in BCM

• Advice for firms on BCM

BCP serves a purpose, better to have a BCP, imperfect as it is, than none…
Crisis Management During Outbreak
Quick Poll
Business Operation Challenges

• Businesses are being required to take on more responsibility
  – Effective communications
  – Provide masks, hand sanitiser
  – Manage work locations
  – More awareness as interact with suppliers, customers etc

• Make decisions about event cancellation and where staff work

• Travel policy

• Increased use of technology to conduct business

• Dust off Business Continuity Plans

• Operate with reduced staff headcount due to enforced leave of absence
Lessons Learned

• **Understand** the threat and how it relates to you

• **Communicate**, communicate & communicate!
  – Clear, timely and stick to the facts
  – Unlikely an existing playbook will cover everything

• **Robust and tested** Crisis Management Plans

• **Seasoned** Crisis Management Team
  – Relevant business leaders

• **Unseen threats** are becoming apparent like Phishing
What being Prepared Really Means

• **Relevant** Pandemic Crisis Management Plan
  – Standardised around the region
  – Tested and exercised

• **Seasoned** Crisis Management Team
  – Carefully selected members
  – Tested and well led

• **Effective Communication**
  – Have plans in place
  – Identify someone in the CMT to be the focus for communication

• Escalate response based on **triggers**
  – WHO or government guidelines may not fit your organisation
  – Be prepared to make wide ranging decisions about business travel, work locations, holiday travel

• **Exercise** your response continually -- Table Top Exercises
Security Risk Management Solutions

1. Dispatch of expert, onsite assistance, embedded member of your crisis management team
2. Providing virtual ongoing crisis support
   - Pandemic Crisis Management Plans
   - Organize, draft and implement emergency preparedness and emergency action plans
4. Crisis Communication Guidance
5. Facilitate tabletop exercises for company leadership and designated response teams
6. Ensure holistic training is in place to respond to the crisis confidently
Unseen Risks and Threats
Quick Poll
Cyber Attack Trends

2020 Top Kroll Incident Response Engagements

- Ransomware
- Email Compromise

These attacks often rely on human weakness and COVID-19 is a perfect opportunity
Ransomware

- Malicious software launched by threat actors to encrypt all user files on a system, then demands ransom payment to decrypt the files.

- Easy preys:
  - Emails
  - Unpatched system vulnerabilities

  » Threat actors take advantage of gaps in systems to gain access.
Ransomware

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
@protonmail.com
or
@tutanota.com

BTC wallet:

Ryuk
No system is safe
Ransomware

Your computer has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - Decryptor

You can do it right now: Follow the instructions below. But remember that you do not have much time

Decryor price

You have 2 days, 19:22:29
* If you do not pay on time, the price will be doubled
* Time ends on Jul 19, 23:03:12

Current price
0.13490081 BTC
≈ 1,300 USD

After time ends
0.26980162 BTC
≈ 2,600 USD

Bitcoin address: [redacted]

INSTRUCTIONS
CHAT SUPPORT

How to decrypt files?

Buy Bitcoins with Bank Account or Bank Transfer
Email Breaches

- Compromise via phishing – Multi-factor Authentication not enabled

- **Post compromise:**
  - Additional phishing messages sent to your contact list
  - *Unauthorised inbox rules* created to redirect messages to hide from your view
  - Learning of your business processes
  - Redirect invoices to bank accounts controlled by threat actors
  - Takeover of your email client software to conduct a complete mailbox data theft
Phishing

This document has been shared with you by [Redacted]

DOWNLOAD/VIEW YOUR DOCUMENT ONLINE
Phishing

**You received 2 new voicemail**

**From:** Office 365 Voice Message Center <.office365.voicemessage@telus.net>

**To:** [Redacted]

**Sent:** March 4, 2019 2:59:01 PM UTC

**Received:** March 4, 2019 9:59:58 AM UTC

**My tags:** Pertinent

---

**Office 365**

**You have (2) New Voicemail messages**

**Dear:** [Redacted]

You received 2 new voicemail messages in your mailbox.

**From:** Wireless Caller (+972-8779-2***)

**Date:** Monday, March 4, 2019 at 09:41:31 AM

**Duration:** 2 Minutes: 35 Seconds

You can get this message via the phone, or listen to the message below.

[Listen To Message Here]

(c) 2019 Microsoft Corporation. All Rights Reserved | Acceptable Usage Policy | Privacy Notice.
Good Afternoon,

Please see below proposal from [Redacted] for your review. https://[Redacted].my.sharepoint.com/o:/g/personal/[Redacted]/EpsyYhWy2cJFkcCvcsZHBbABNzbaCVKUCujOT1XxqLH8kA?e=4cEN1N

Kindly let me know if you have any concerns.

I await your feedback

Warm regards, Andrea

Andrea [Redacted] Ltd.
tel: [Redacted] 7399
fax: [Redacted] 8499
COVID-19 Threat

Watch Out for Coronavirus Phishing Scams
At least one email campaign is preying on fears by claiming to offer info about the Wuhan coronavirus.

Singapore Specialist: Corona Virus Safety Measures

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms: Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [Name]
Specialist [Affiliation]
COVID-19 Threat

Scammers are pretending to conduct contact tracing to procure information from S’pore victims

SINGAPORE - The Ministry of Health (MOH) has stated that it is contacting individuals for contact tracing in the light of the coronavirus outbreak, but will not ask for financial details during these calls.

This comes after a message warning of a contact tracing phone scam was widely circulated on social media.

"MOH is conducting contact tracing to identify individuals who had close contact with the confirmed cases of novel coronavirus," the ministry said in a Facebook post on Saturday (Feb 8).
COVID-19 Threat

Nasty Trickbot malware exploits people’s Coronavirus fears

By Matt Hanson  5 days ago

Italian email addresses targeted

Malicious hackers are using people’s fear of the Coronavirus to spread malware, known as Trickbot, by emailing an official-looking message that claims to contain a document listing some helpful precautions. Instead, it contains an infected Word document.

The email has been sent to Italian email addresses. Italy has been one of the most affected countries by Coronavirus, and the spam emails are preying on its residents’ understandable concern about the disease.
Practical Recommendations

• **Be cyber smart**
  – Regular trainings
  – Test employees’ level of awareness
  – Share experiences

• **Think before you click!**
  – Be suspicious of messages from people you do not know and/or attachments you do not expect

• Enable **multi-factor authentication** on your accounts

• Keep operating systems, software, and anti-virus protection **up to date**

• Request to **call people back** if they request information from you
Q&A session
About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, disputes and investigations, cyber security, claims administration and regulatory issues. We work with clients across diverse sectors on matters of good governance and transparency. With Kroll, the leading global provider of risk solutions, and Prime Clerk, the leader in complex business services and claims administration, our firm has nearly 4,000 professionals in 25 countries around the world. For more information, visit www.duffandphelps.com.

Koh Sin Yee
Director
Compliance Regulatory Consulting
Duff & Phelps
sinyee.koh@duffandphelps.com

Simon Ashenden
Associate Managing Director
Security Risk Management
Kroll, a division of Duff & Phelps
simon.ashenden@kroll.com

David Klopp
Associate Managing Director
Cyber Risk
Kroll, a division of Duff & Phelps
david.klopp@kroll.com