

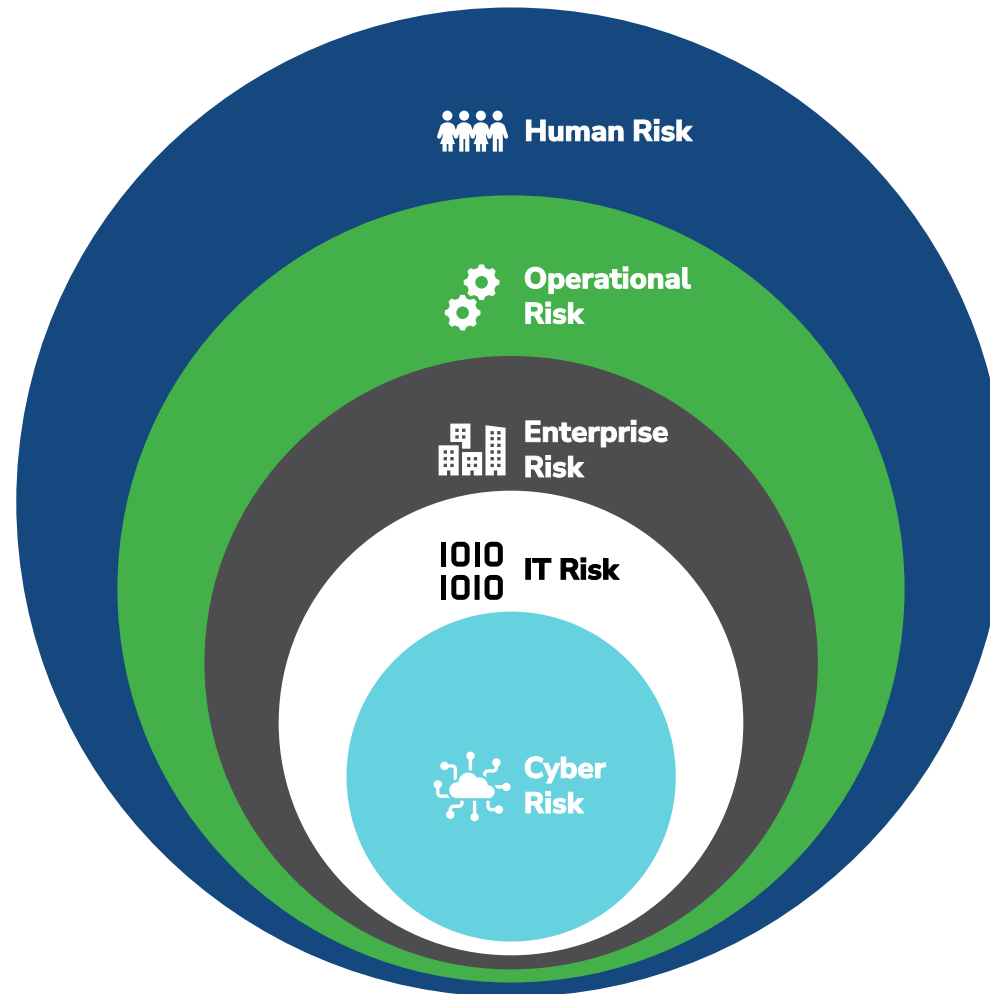


Enhancing Security Awareness via Simulation

Neo Lam

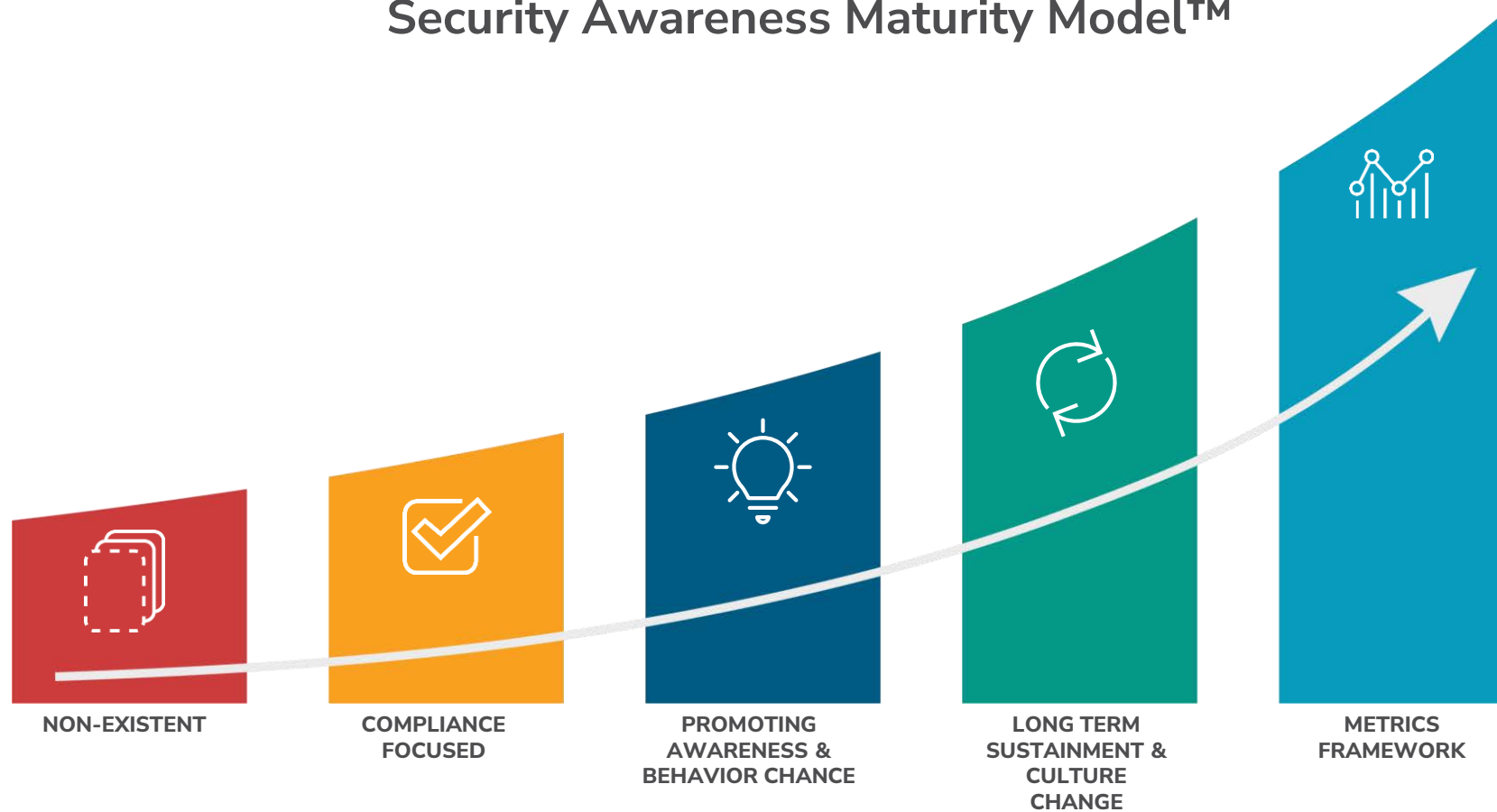
Associate Managing Director, Kroll Cyber Risk APAC

Layers of Risk Management



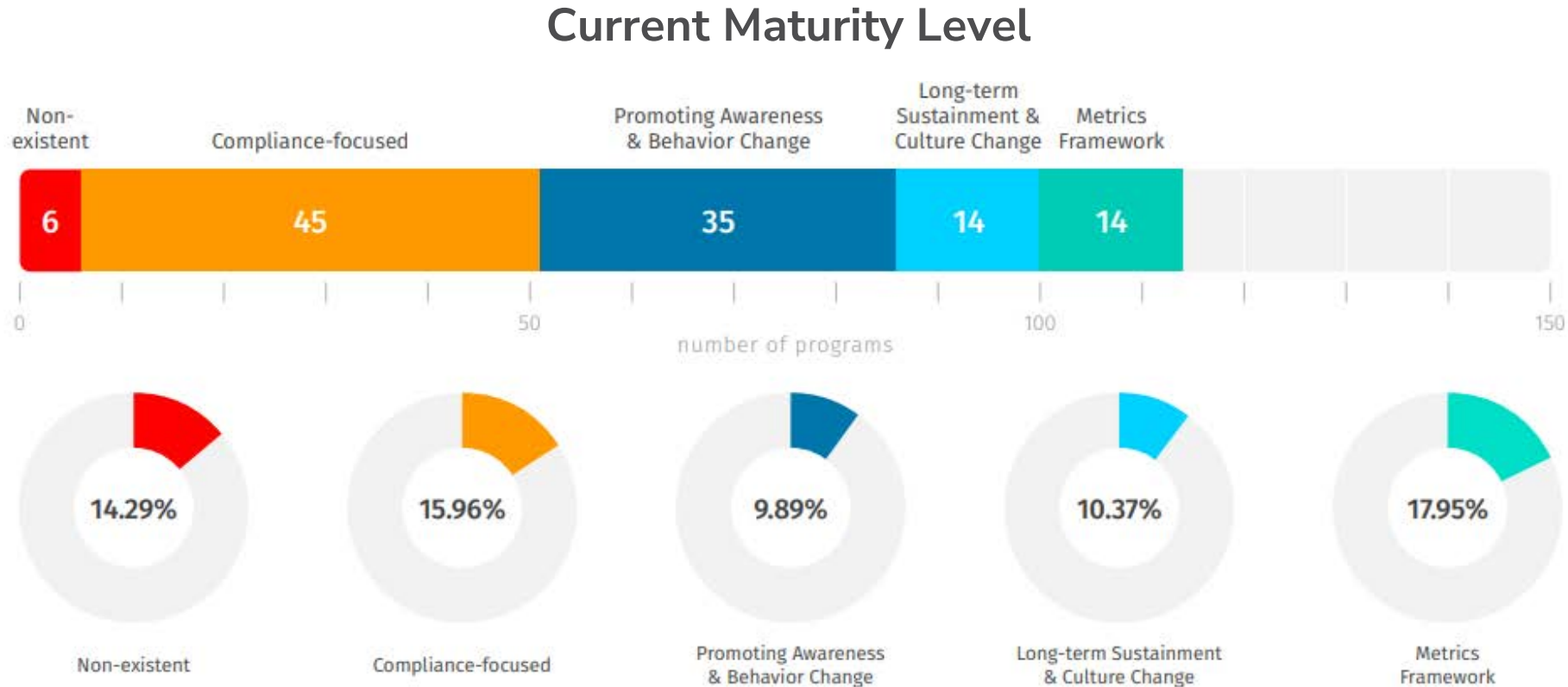
The Maturity Model from SANS Security Awareness

Security Awareness Maturity Model™



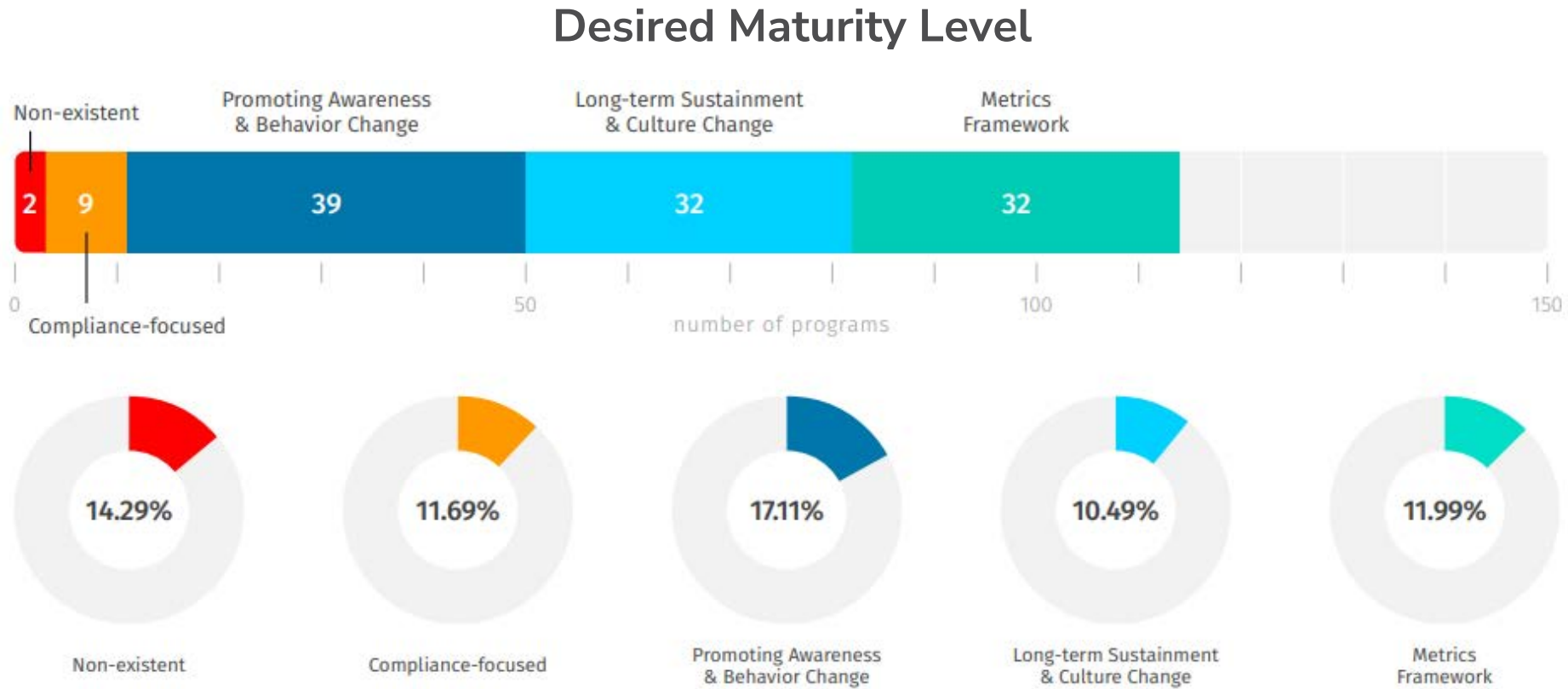
Source: <https://www.sans.org/security-awareness-training/resources/maturity-model/>

Maturity Level of Organisation's Security Awareness Program from SANS Security Awareness



Source: <https://go.sans.org/lp-wp-2022-sans-security-awareness-report>

Maturity Level of Organisation's Security Awareness Program from SANS Security Awareness



Source: <https://go.sans.org/lp-wp-2022-sans-security-awareness-report>

What May Happen if Security Awareness Maturity Level is Low?

Mock Scenario



ABC Healthcare

Reputable multi-national healthcare service provider with offices and hospitals in Hong Kong, Japan, Philippines and Singapore.

All ABC Healthcare's computers have been installed with antivirus. Furthermore, ABC has engaged a service provider for the managed security operations centre (MSOC) service to help them monitor the log record and security information and event management (SIEM).

From time to time, ABC Healthcare will receive false-positive reports from the MSOC partner, which is rather common, and no further action would be taken.

The healthcare company has insurance coverage, but no incident response retainer.

Mock Scenario

● — Monday

— Morning

ABC Healthcare's MSOC reported there were some abnormal log records over the weekend from department.

After screening, antivirus scans returned a negative result, and everything seemed normal.



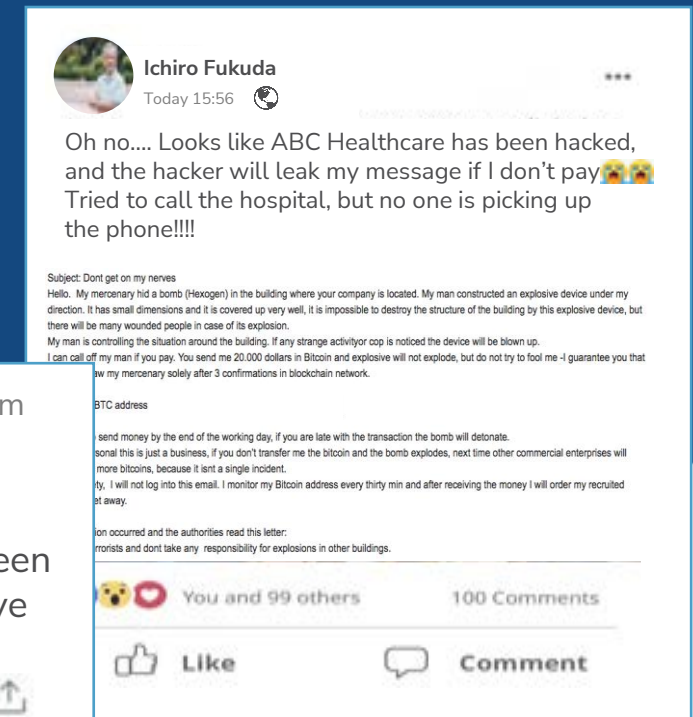
Mock Scenario

● — Monday

— Morning

— 17:00

Shortly after, many patients of ABC Healthcare started posting on social media about receiving emails threatening to disclose their medical records and demanding bitcoin payments.



Mock Scenario

● — Monday

— Morning

— 17:00

— 23:30

In the evening, news media was reporting this situation discussed and posted on the social media threads.



Mock Scenario

● — Monday

— Morning

— 17:00

— 23:30

— 23:35

Have you read the news?
Social media is trending
we're being hacked.... Can
you pls check?

Let me ask the team to do a
health check on the system
ASAP

Here is the link to the twitter
page that is trending
<https://twitter.com/home?lang=zh-Hant>

Thanks, let me read into it. I
have also requested MSOC
to stay alert tonight.

CIO received text
messages from its PR
representative.

CIO immediately asked
the MSOC to look into the
situation and stay alert.
The MSOC partner
lowered the thresholds of
sending alerts.

Mock Scenario

- — **Monday**
 - Morning
 - 17:00
 - 23:30
 - 23:35
- — **Tuesday 11:00**

CIO received multiple alerts from MSOC partner about suspicious activities from 5 endpoints in the Hong Kong office. They were not able to identify the root cause.




The company immediately engaged with a local incident response service provider, BBX, which quoted the lowest cost. Within 30 minutes, they agreed on the price for the engagement of the 5 endpoints.

The IT team took BBX's advice to isolate the computers and terminate the connection between Hong Kong office and other offices in the region. The incident response service provider collected the hard disk from the office to determine the root cause.

Mock Scenario

- — Monday
 - Morning
 - 17:00
 - 23:30
 - 23:35
- — Tuesday 11:00
- — Wednesday 09:15

[Urgent] Cyber Attack

 Kang, Ho
To:  Kang, Ho
Retention Policy Email (11 years)
 Default Outlook

Expires: 8/23/2033

 Reply  Reply All  Forward 

Fri 8/26/2022 10:11 AM

Dear all,

I would like to bring to your attention our offices in Hong Kong, Singapore, Japan and the Philippines have been affected by ransomware attack. Around 1,000 computers are reported to have been affected.

@Information Department – don't we have already have AV and MSOC in place, if so, why are we still being hacked?

Meanwhile, I have also noticed we have already engaged with an IR service provider yesterday, and isolated all the computers, but why has the situation worsen after these actions? How was the vendor chosen? Is the vendor able to support all the locations we cover?

@Legal Department – please check with the insurance company on this matter. Is it easier if we just pay the ransom, after all, these are our patients' personal data?

Best regards,
Albert Fung

CEO

CEO

Albert Fung
Best regards

Mock Scenario

- — **Monday**
 - Morning
 - 17:00
 - 23:30
 - 23:35
- — **Tuesday 11:00**
- — **Wednesday 09:15**
- — **A few days later**

Given the number of over 1,000 endpoints involved across multiple markets, the appointed local incident response service provider was not able to handle such demand.

ABC Healthcare had to terminate and engage a regional service provider, CED, to handle the incident.

Mock Scenario

- — **Monday**
 - Morning
 - 17:00
 - 23:30
 - 23:35
- — **Tuesday 11:00**
- — **Wednesday 09:15**
- — **A few days later**
- — **Few weeks later**

After several weeks, the system was finally recovered. Unfortunately, a class-action lawsuit was filed by the affected customers. However, CED did not provide Breach Notification or Litigation Support services.

To make things worst, ABC Healthcare was notified by its insurance carrier that the first IR company, BBX, that it had engaged with was not on the list of approved vendors.

Therefore, the cyber insurance claim may be declined due to one of the common exclusions – error & omission.

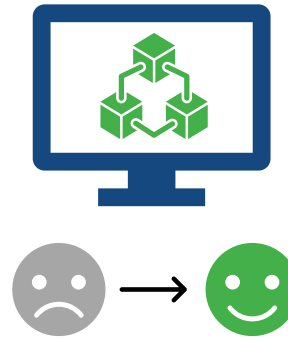
Key Elements for Enhancing Security Awareness



Stakeholder
Acceptance



Leadership
Support



Simulation
Experience



Cyber Crisis
Management
Training

Cyber Crisis Management Training

Cyber Crisis Management Training Should Be



Inclusive – caters to the full set of stakeholders - both technical and management.



Relevant – collects and analyses customized information to ensure the scenario targets useful data points and have proven experts in complementary fields such as security risk management and operational resilience – enabling us to craft a well-rounded scenario.



Impactful – provides relevant learning outcomes and crisis management practice to all participants.



Engaging and Fun – highly interaction by leveraging video content, web pages, live social media etc.



Analytical – post-event report provides a detailed level of analysis, sector-wide and institution-specific.

A Simulation Built for specific environment

Utilise knowledge of the information and technology environment, and the understanding of SME situations to maximise the value of the exercise for participants



PEOPLE AND PROCESS

- Crisis Management Team
- Business Continuity Plans
- Incident Playbooks/ SOPs
- IT Disaster Recovery Plans
- Training and awareness



RELEVANT THREATS

- Ransomware
- State sponsored or corporate espionage
- Hacktivists
- Coerced Staff
- Supply Chain Compromise



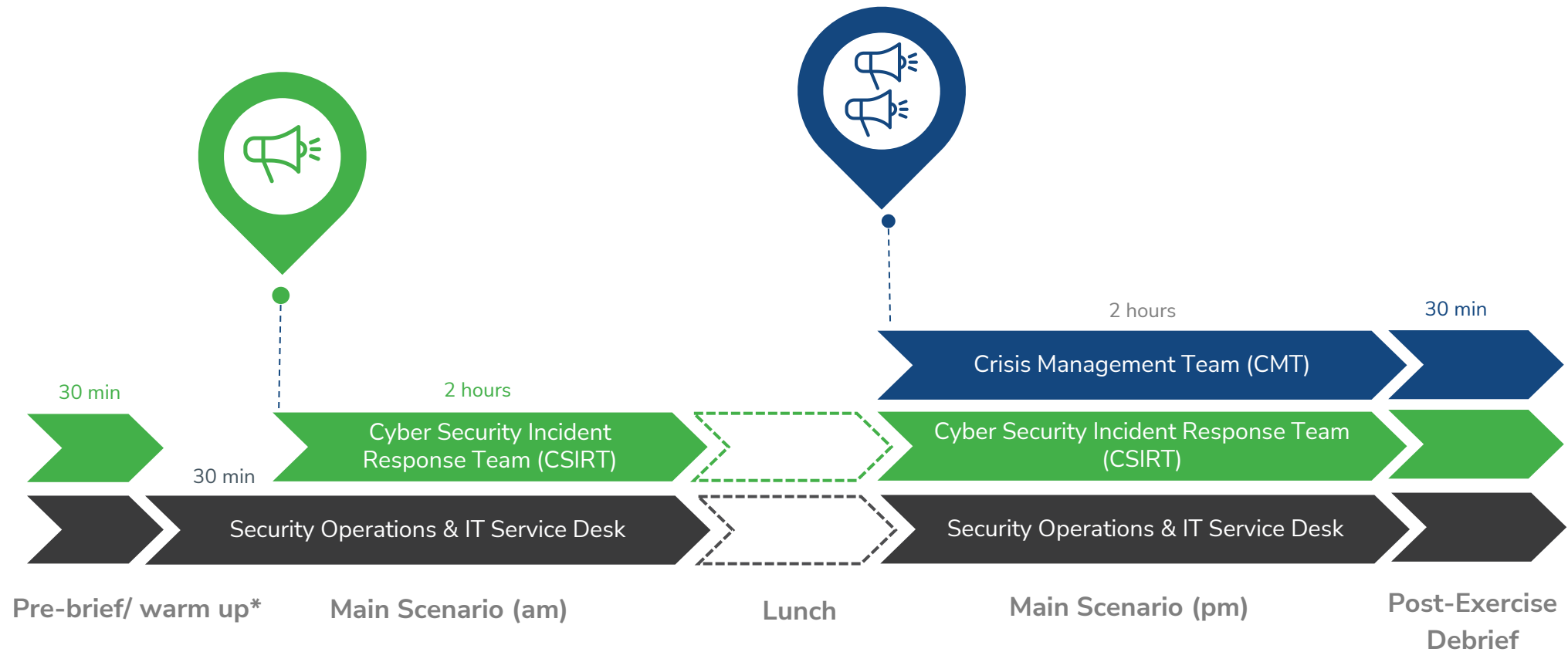
INFORMATION AND TECHNOLOGY

- Critical applications
- Networks
- Backups
- Cloud systems
- Technical security controls – PAM, firewalls, MDM, SIEM, XDR, EUBA, etc.

Cyber Crisis Management Training Preparation Phases



Example Agenda



Delivery Method



In Person

- Purpose-built Technology Platform
- Physical (paper-based)
- PowerPoint driven



Remote / Anywhere

- Purpose-built Technology Platform
- Work-from-home Environment



For more information, please contact:



Neo Lam

Associate Managing Director, Cyber Risk

+852 6011 5215

Neo.lam@kroll.com

About Kroll

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorized and regulated by the Financial Conduct Authority. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.

© 2022 Duff & Phelps, LLC. All rights reserved. Kroll is a trade name for Duff & Phelps, LLC and its affiliates.