Security for the C-Suite
Workshop Part I

Tobin Joseph

01/12/2023

Agenda

General Security Trivia Questions

The Value Proposition of a Security Posture and a Response Strategy

Strategic Planning for the Value Proposition

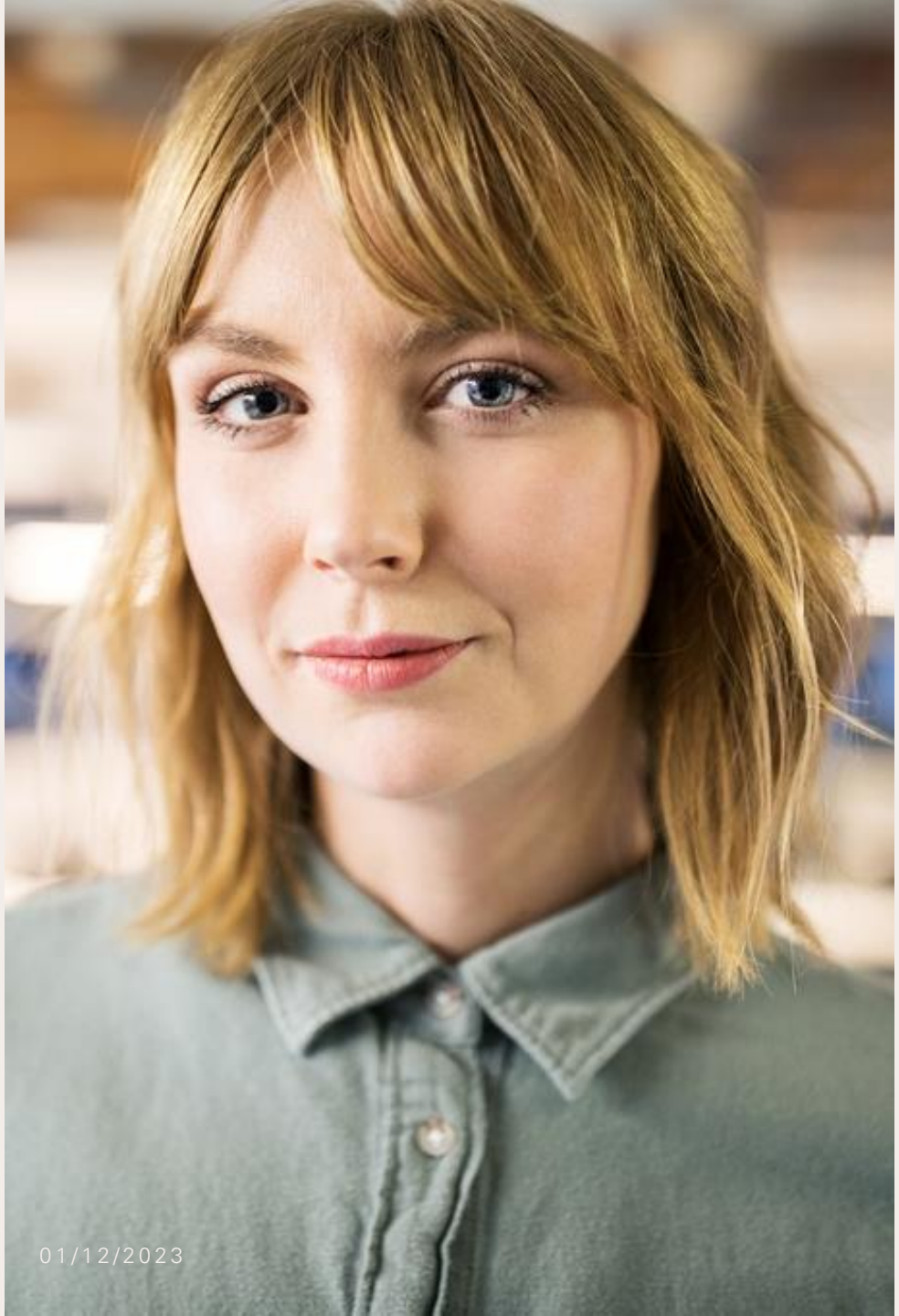
Internal Activities Before a Cyberattack

External Activities Before a Cyberattack

Internal Activities After a Cyberattack

External Activities After a Cyberattack

Group Exercise



Vulnerability

What do you think is the most vulnerable risk element your organization has from a security/cybersecurity standpoint?

Vulnerability

The most vulnerable risk element in your organization are your employees, starting with the CEO!

Vulnerability

"Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 ($243,000) in March (2019) in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking. The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm's German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive to pay within an hour, according to the company's insurance firm, Euler Hermes Group SA."

- Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case, Catherine Stupp at Catherine.Stupp@wsj.com. Wall Street Journal - 2019 Dow Jones & Company, Inc.

Vulnerability

"95% of all attacks involve some form of social engineering."

-Inc. 2017, USA

“82% of breaches against businesses involved a human element, through issues like error and social engineering.”

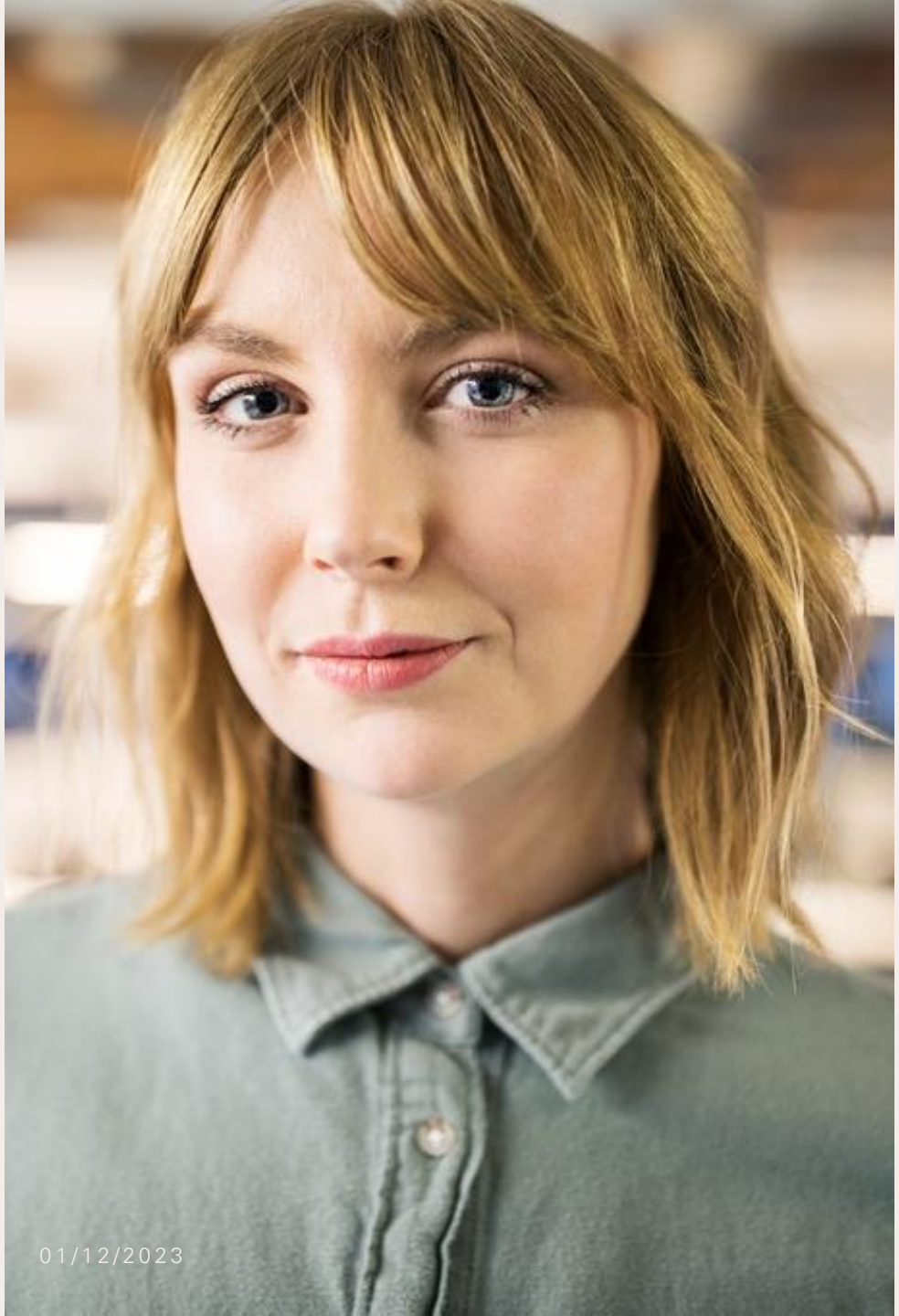
-The Latest 2022 Cyber Crime Statistics (updated December 2022)

AAG, UK

Vulnerability

“Cybercriminals aren't only targeting your employees; now they're also after the C-suite. The number of reported data breaches continued increasing exponentially this year, up 17% from 2020. Even more alarming is that a growing number of these attacks are aimed at high-level accounts. Business email compromise scams that are skillfully crafted to trick even the savviest of victims are on the rise, resulting in losses of $1.8 billion in 2020, according to the FBI's Internet Crime Report, and reaching unprecedented levels since. Account takeover attempts rose a staggering 671% in the third quarter of 2021, according to a study by one cloud email security provider.”

-Why Security Awareness Training Should Begin in the C-Suite, Ashley Rose, CEO and Co-Founder, Living Security, January 2022



Worst Risk

What do you think is the most significant risk to your organization from a security standpoint? What is the works that can happen?

Worst Risk

Your most significant risk is going out of business due to a cybersecurity attack!

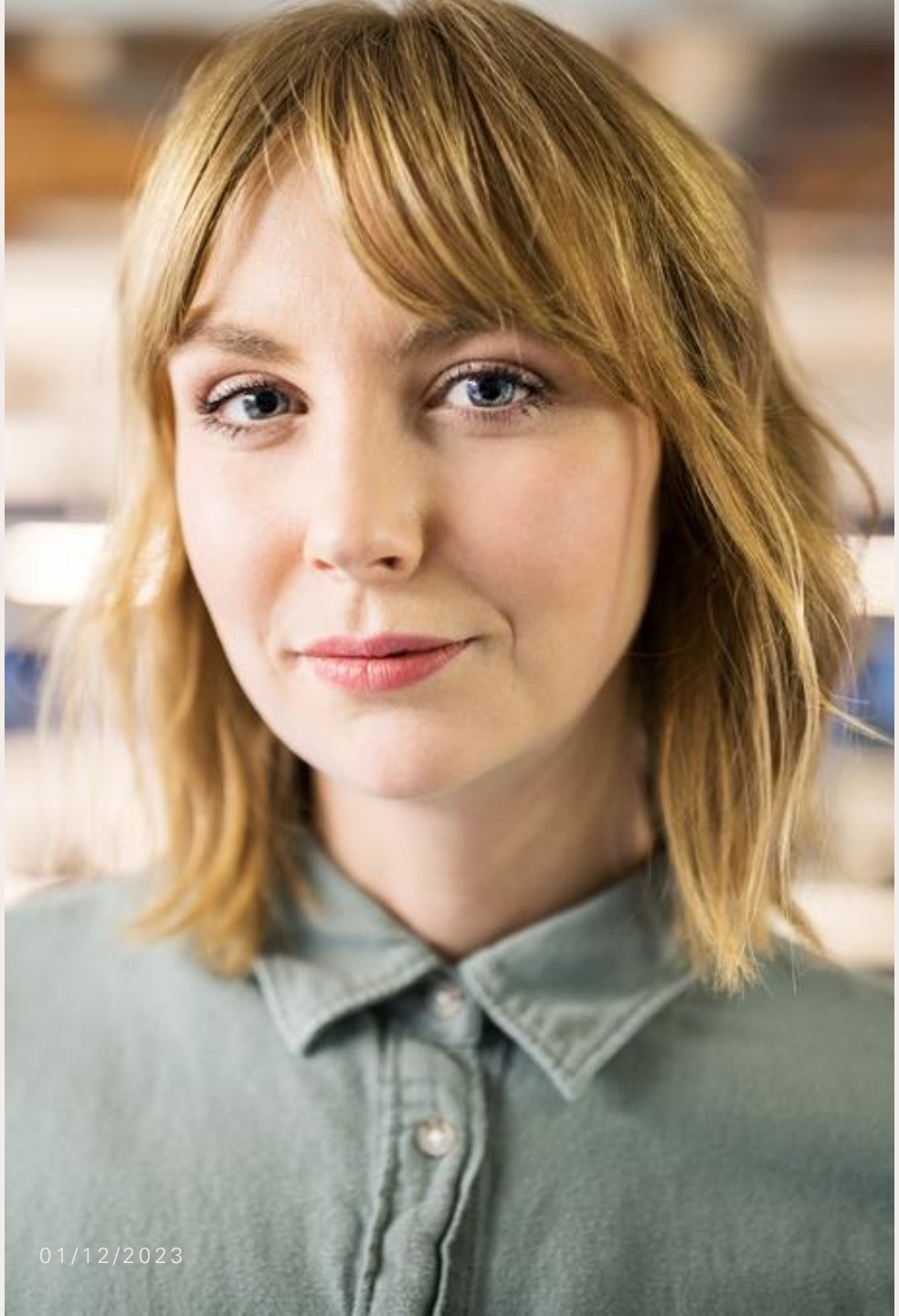
Worst Risk

"60 Percent of Companies Fail in 6 Months Because of a cyberattack."

-Inc. 2017, USA

"In a 2022 case study covering the US, Canada, UK, Australia, and New Zealand, 69% of the respondents were fearful that a successful cyber attack could put their SMB out of business entirely."

-The Latest 2022 Cyber Crime Statistics (updated December 2022) AAG, UK



Threat Origins

Where do you think most threats in security to your organization are more likely to come from?

Threat Origins

Most threats in security to your organization are more likely to come from your supply chain.

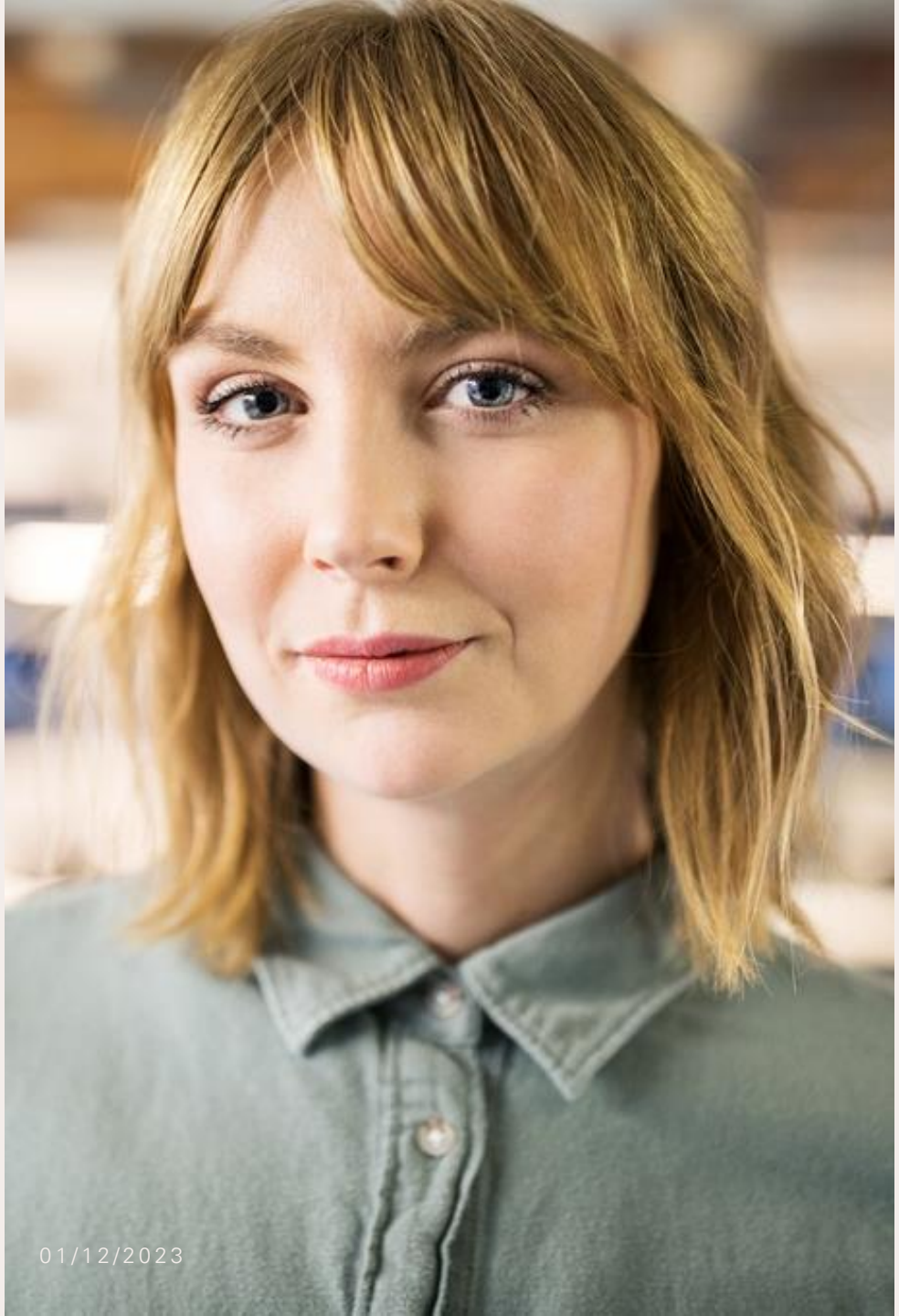
Threat Origins

“Supply chains are becoming increasingly interconnected and complex as technology improves. However, security vulnerabilities in one business can expose partners they are connected with. Cybercriminals are targeting these vulnerabilities, with up to 40% of cyber threats now occurring indirectly through the supply chain.

...

Recent research also highlights the worry of C-Suite executives about vulnerabilities in the supply chain. When 900 companies were asked what they thought were the most likely types of cyber attacks on their business, 60% responded with supply chain attacks. This is the same as DDoS attacks, ahead of cyber espionage (59%) and APT (57%), but less than ransomware and data theft (66%). “

-The Latest 2022 Cyber Crime Statistics (updated December 2022)
AAG, UK



No Threats

Can we completely eliminate the threats to our organizations?

No Threats

Eliminating threats is impossible

No Threats

"Eliminating threats is impossible, so protecting against them without disrupting business innovation and growth is a top management issue."

–James Kaplan, Shantnu Sharma, and Allen Weinberg
Business Technology Office, 2011 McKinsey & Company

"76% of respondents in a 2022 case study covering the US, Canada, UK, Australia, and New Zealand say their organization has suffered at least 1 cyber attack this year. This is a large increase over the 55% figure in 2020."

-The Latest 2022 Cyber Crime Statistics (updated December 2022)
AAG, UK

No Threats

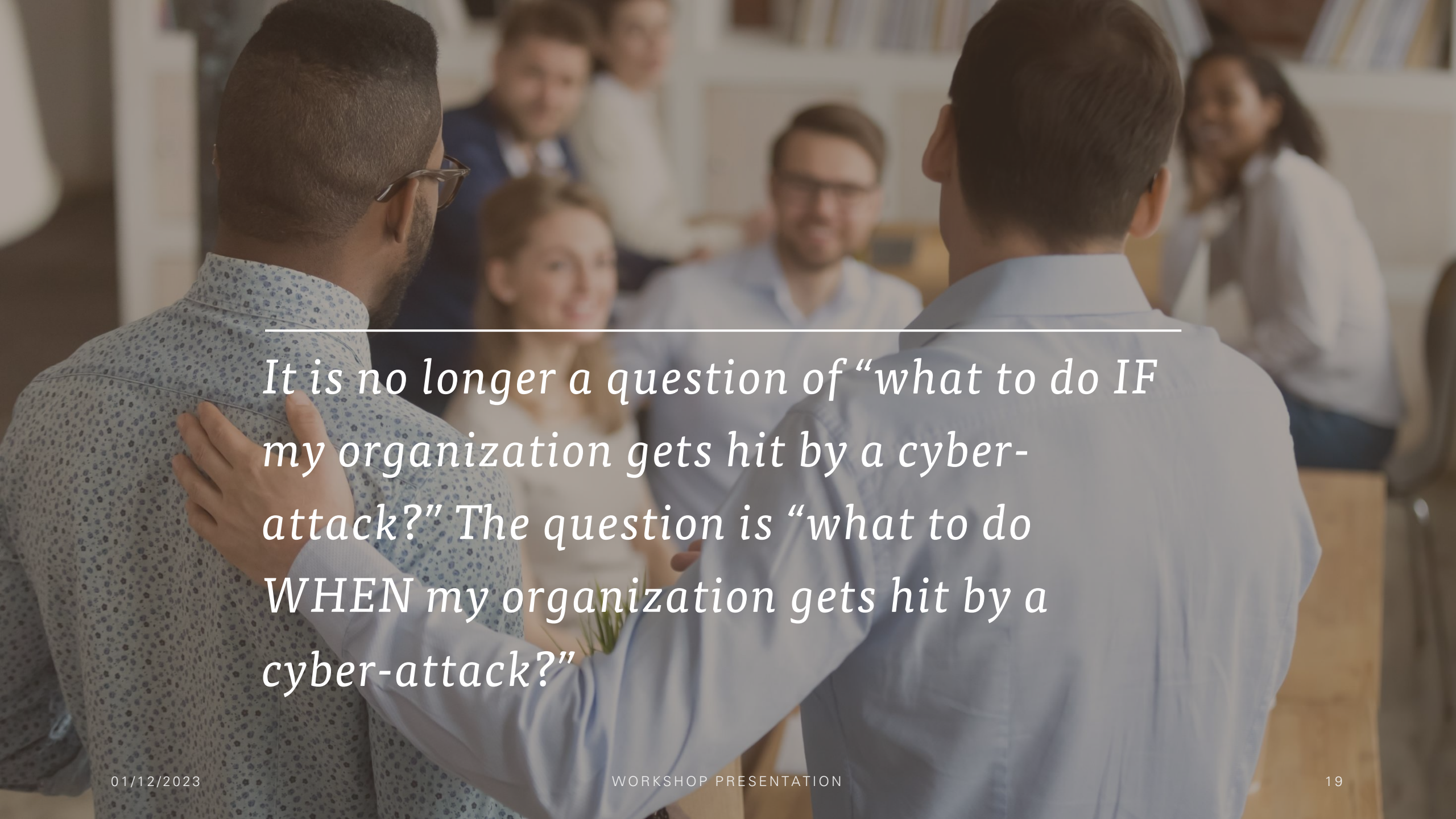
"According to the Identity Theft Resource Center, data breaches rose 17% between 2020 and 2021. And 67% of survey respondents report that their organizations experienced between one (1) and 10 cyber incidents or breaches over the past year—and an additional 15% say they experienced 11 to 15 incidents." (total of 82% of organizations reported at least one incident)

-Cybersecurity in a post-pandemic world: A focus on financial services, Deloitte Global, 2022

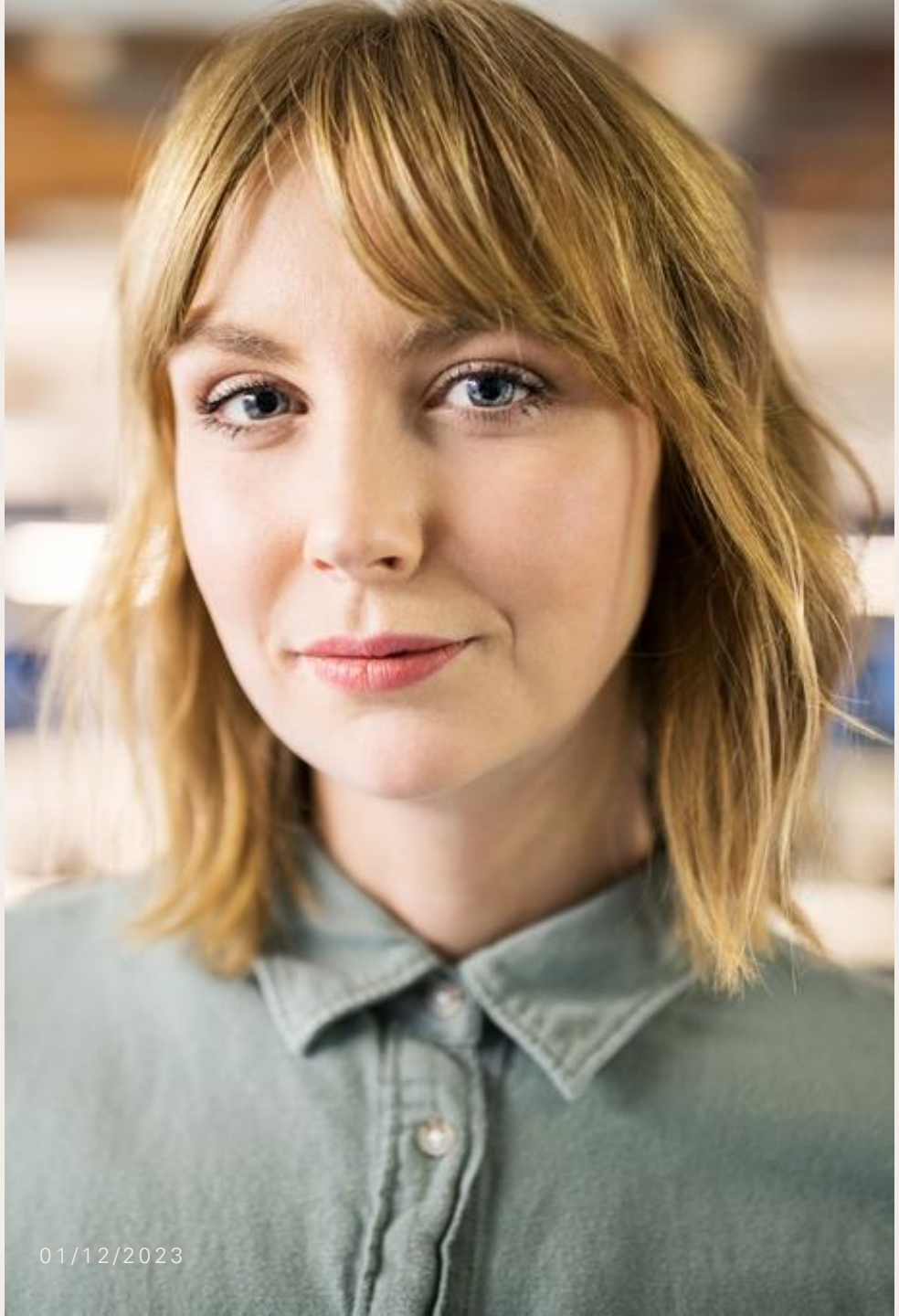
No Threats

“We live in a world...of massive connections where that critical infrastructure that we rely upon is all underpinned by a technology ecosystem that unfortunately has become really unsafe. We cannot have the same sort of attacks on hospitals and school districts that we've been seeing for years. We have to create a sustainable approach to cyber safety, and that's the message that I'm bringing to CES.”

-Director Jen Easterly, Cybersecurity and Infrastructure Security Agency, USA at CES 2023 in Las Vegas, NA interview with Yahoo Finance 01/05/2023



It is no longer a question of "what to do IF my organization gets hit by a cyber-attack?" The question is "what to do WHEN my organization gets hit by a cyber-attack?"



Responsibility

Who is responsible for security/cybersecurity in your organization?

Responsibility

The CEO, the Board of Directors, and the C-Suite Executives.

Responsibility

"Cybersecurity responsibilities are owned by the CEO and the top management who have the authorities to make decisions across organizations"

-The CISO Role: a Mediator between Cybersecurity and Top Management, No. 2 (2022): NOKOBIT Norsk konferanse for organisasjoners bruk av IT, Norway

"CEOs need to embrace good corporate cyber responsibilities."

-Director Jen Easterly, Cybersecurity and Infrastructure Security Agency, USA at CES 2023 in Las Vegas, NA interview with Yahoo Finance 01/05/2023

Security Posture and Response Strategy

Value Proposition

Manage the risk of going out of business due to a cyberattack.

Avoid the high cost of noncompliance (regulatory fines are just the beginning).

Gain and maintain the trust and loyalty of your customers, partners, stakeholders, and employees.

"

Make Cybersecurity a Strategic Asset

By elevating cybersecurity from an operational necessity to a source of opportunity, leaders can boost resilience and business advantage."

-Manuel Hepfer And Thomas C. Powell, Reboot Your Strategy, MIT Sloan Management Review, Fall 2020

Strategic Planning for the Value Proposition of a Security Posture and Response Strategy

The Strategic Planning to attain this Value Proposition encompasses four main areas divided into activities before (security posture) and after (response strategy) a cyberattack (because is not a question of IF, is a question of WHEN) that focuses on stakeholders inside and outside the company, creating resilience without disrupting business innovation and growth (inside) and creating a business advantage (outside).

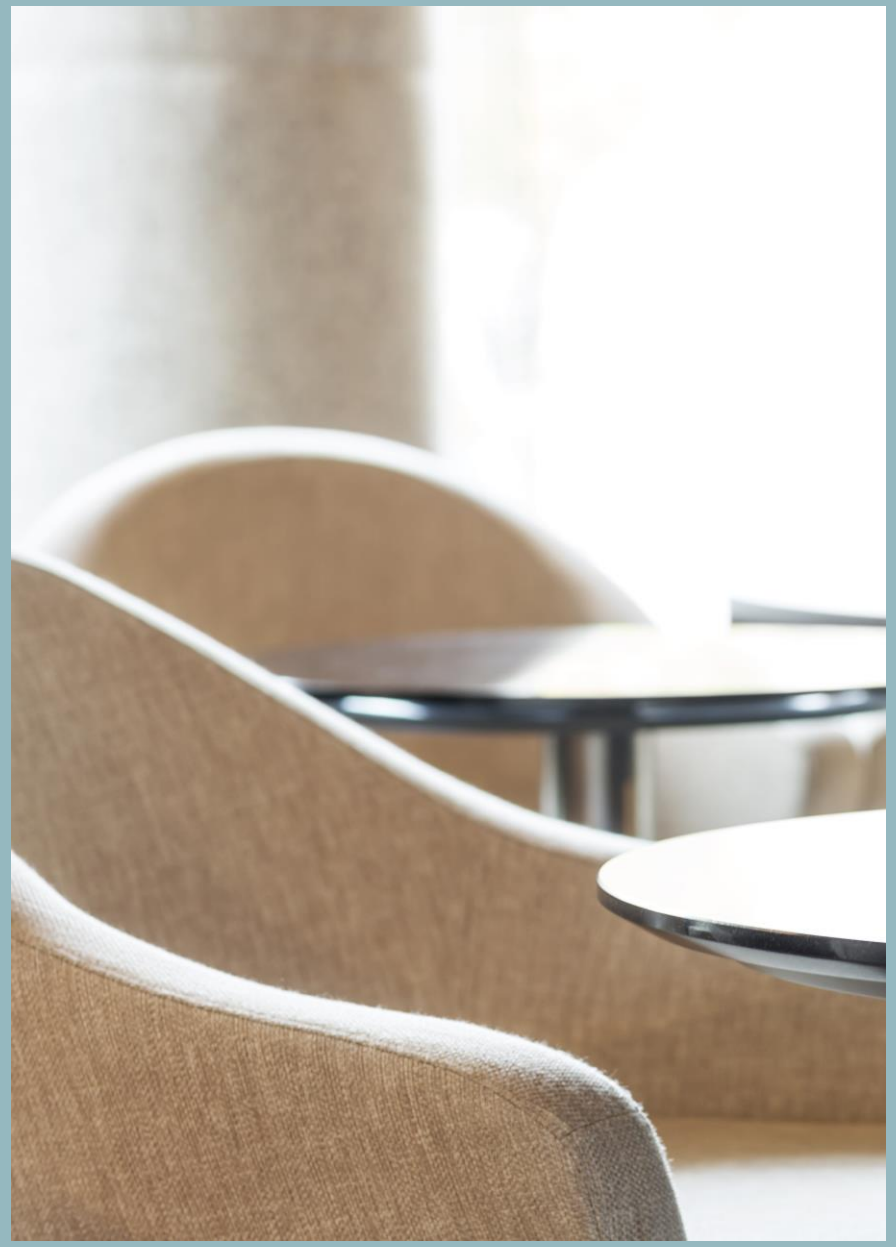
By 2025, it is estimated that 60% of organizations will use cyber security risk as a key factor when determining transactions and business engagements with third parties.

Security Posture

- Internal Activities Before a Cyberattack
- External Activities Before a Cyberattack

Response Strategy

- Internal Activities After a Cyberattack
- External Activities After a Cyberattack



Before an Attack

Internal Activities

Suggested Internal Activities Before a Cyberattack

Prepare your C-suite Team and Board of Directors with the basic tools necessary to assess, manage and monitor the existential risks posed by cyberattacks.

Suggested Internal Activities Before a Cyberattack

Have a security team to help to prepare and execute the human and technological aspects necessary to protect the attack surface of your organization.

Suggested Internal Activities Before a Cyberattack

Embed in your organization's culture and values the need to care for security as a survival issue for the organization. Train and test the members of your organization, from the Board of Directors, The C-suite Team all the way to the bottom.

Suggested Internal Activities Before a Cyberattack

Create/review internal policies, procedures, and audit processes for securing your organization to reduce the attack surface as much as possible. Create/review internal policies, procedures, and audit processes for securing your organization to reduce the attack surface as much as possible.

Suggested Internal Activities Before a Cyberattack

Identify the most critical business processes and data that your organization needs to function. Design a backup strategy as part of your response plan for when a cyberattack comes.

Suggested Internal Activities Before a Cyberattack

Define Key Risk Indicators and Key Performance Indicators to be used in measuring the security posture you design.

Suggested Internal Activities Before a Cyberattack

Make a monthly review at the Top Management Level of these KRIs and KPIs to monitor progress, organizations' security health, and new threats emerging.

Suggested Internal Activities Before a Cyberattack

Make drills/exercises of your backup strategies and response plans for when a cyberattack occurs. Make sure these work before an attack comes.

Suggested Internal Activities Before a Cyberattack

Commit to a transparency policy to communicate the current status of your security posture and response strategy.

Before an Attack

External Activities

Suggested External Activities Before a Cyberattack

Communicate to your principal stakeholders not involved in day-to-day operations (shareholders, members, etc.) the current state of your security posture and response strategy (include these at least in your Annual Report).

Suggested External Activities Before a Cyberattack

Have contracts with external suppliers and recruit personnel as needed to support your security posturing and have the resources in place for a response to an attack.

Suggested External Activities Before a Cyberattack

Transfer some of the risks using cyber security insurance.

Suggested External Activities Before a Cyberattack

Have your organization make relations with the cybersecurity community to keep up with current trends, advancements in technology, and threats.

Suggested External Activities Before a Cyberattack

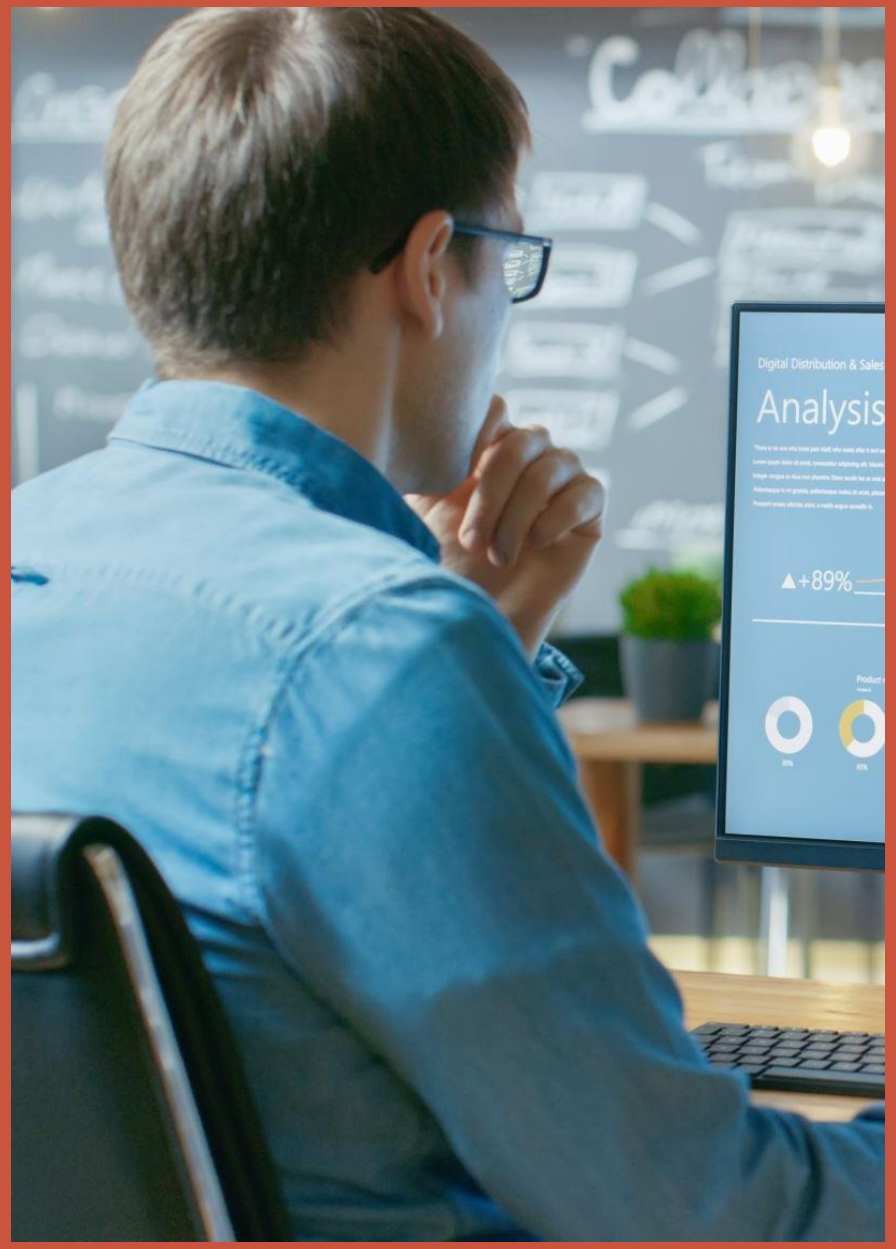
Examine the cyber security risk posed to your organization by your external business partners, suppliers, and clients and use it as a key factor in determining your interactions with them.

Suggested External Activities Before a Cyberattack

Make relations with applicable regulators, external auditors including external testers (like penetration testing), government agencies, and business organizations to help you with your security posture and to communicate it to them.

Suggested External Activities Before a Cyberattack

Once you have your security posture in place, with some audits and maybe external partners verifying your cyber security risk, communicate this to your clients/partners to build and keep their trust in doing business with you.



After an Attack

Internal Activities

Suggested Internal Activities After a Cyberattack

Inform your Board of Directors, C-Suite Team, and employees of the attack.

Suggested Internal Activities After a Cyberattack

Start containment of the attack to avoid spread as soon as you know about it. This should be the first part of your response to recover your operations.

Suggested Internal Activities After a Cyberattack

Have your security team and personnel assigned to deal with the crisis along with the external resources start to perform the planned actions.

Suggested Internal Activities After a Cyberattack

Make an assessment of the impact on your operations, especially the critical processes and data.

Suggested Internal Activities After a Cyberattack

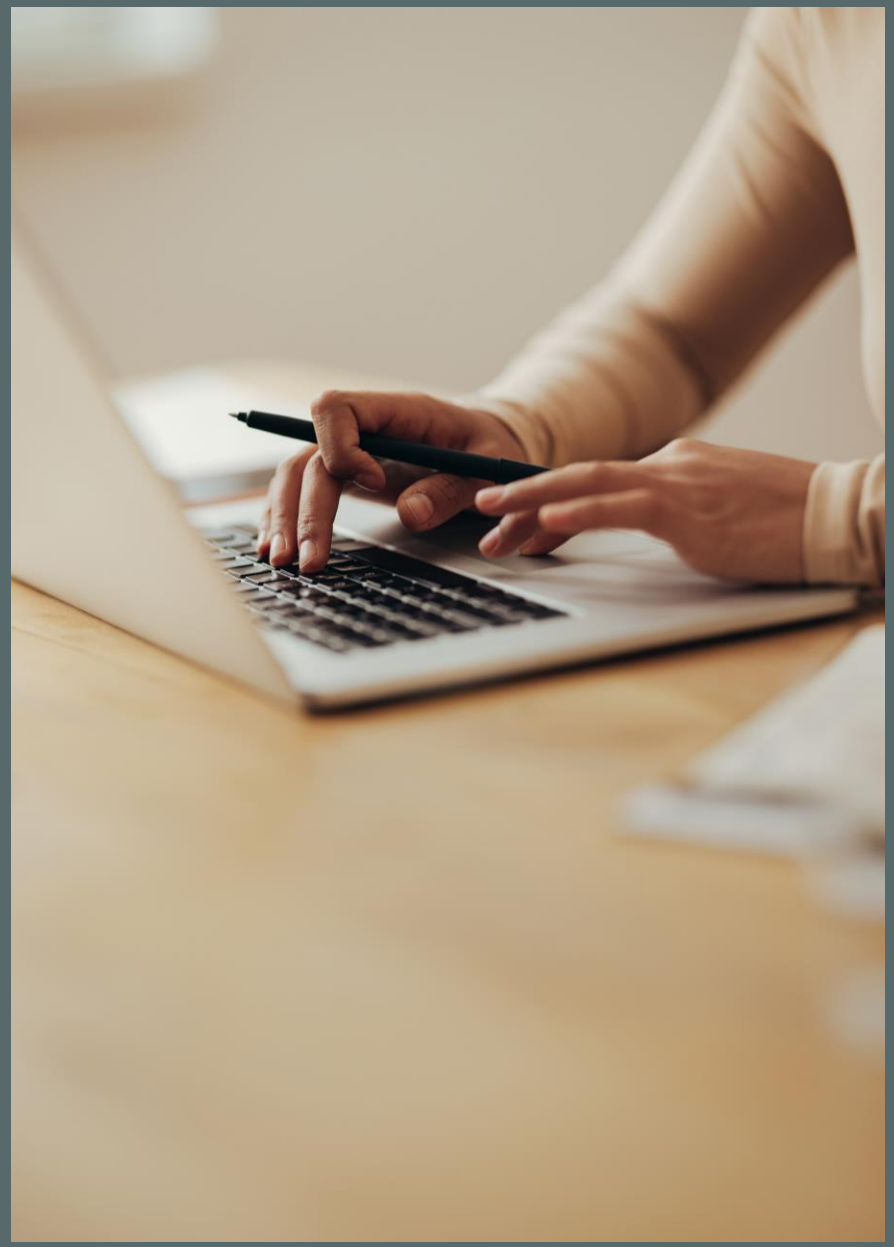
Start your backup strategies and response plans according to the areas affected.

Suggested Internal Activities After a Cyberattack

Monitor the progress of the execution of the backup strategies and response plans on the continuation of operations and adjust actions and teams as necessary.

Suggested Internal Activities After a Cyberattack

Make an assessment of the damage caused by the attack and what extra actions needed to be done related to external stakeholders.



After an Attack

External Activities

Suggested External Activities After a Cyberattack

Make transparent communications to designated authorities (FBI, JOD, etc.), as they might be able to help you in the response.

Suggested External Activities After a Cyberattack

Communicate to your principal stakeholders not involved in day-to-day operations (shareholders, members, etc.) the incident and keep them informed of the consequences and progress in the response.

Suggested External Activities After a Cyberattack

Communicate with your business partners, suppliers, clients, and competitors. You might be surprised by the help you can get from your competitors.

Suggested External Activities After a Cyberattack

Manage the public response to the attack with a crisis management public relations specialist.

Suggested External Activities After a Cyberattack

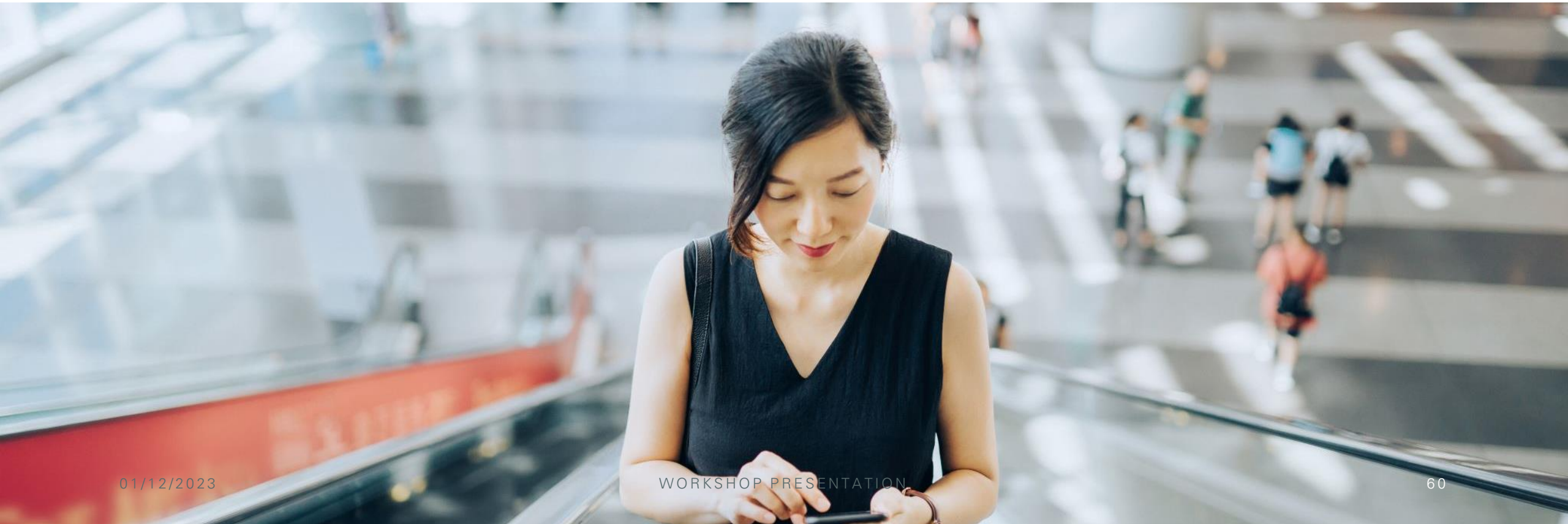
Try to get a feeling of how your clients are responding to the incident.

Suggested External Activities After a Cyberattack

If you have investors, keep an eye on their feelings and responses in the markets.

Suggested External Activities After a Cyberattack

Initiate any compliance report and client support activities needed based on the type of attack (services/products not reaching clients, third-party data stolen like personal, financial, or health-related data, public security issues due to the attack on your organization, etc.)



IMPORTANT

The Strategic Planning for all these activities before and after a cyberattack must be completed as soon as possible before a cyberattack occurs (and there is at least a 76% probability that your organization will be hit by a cyberattack during this year, extrapolating last year's data).

Exercise

What is the current security posture and response strategy of your organization?