Security for the C-Suite:
How to build a good Security Team

Workshop Part II

Tobin Joseph

01/12/2023

Agenda

Security Posture: Comments

Security is an organization-wide responsibility

Strategic Planning to build a good security team: SWOT Analysis

Skills assessment of your current workforce

The Chief Information Security Officer (CISO)

Your current economic context

Skill areas that your analysis might include

Group Exercise

Security Posture: Comments

Your C-Suite

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.

We encourage all your C-Suite Team and the Board of Directors to take this workshop to prepare themselves to tackle security as an opportunity for strategic growth and resilience.

Cybersecurity Insurance

"In a 2022 case study covering the US, Canada, UK, Australia, and New Zealand, just 30% of the respondents have cyber insurance."

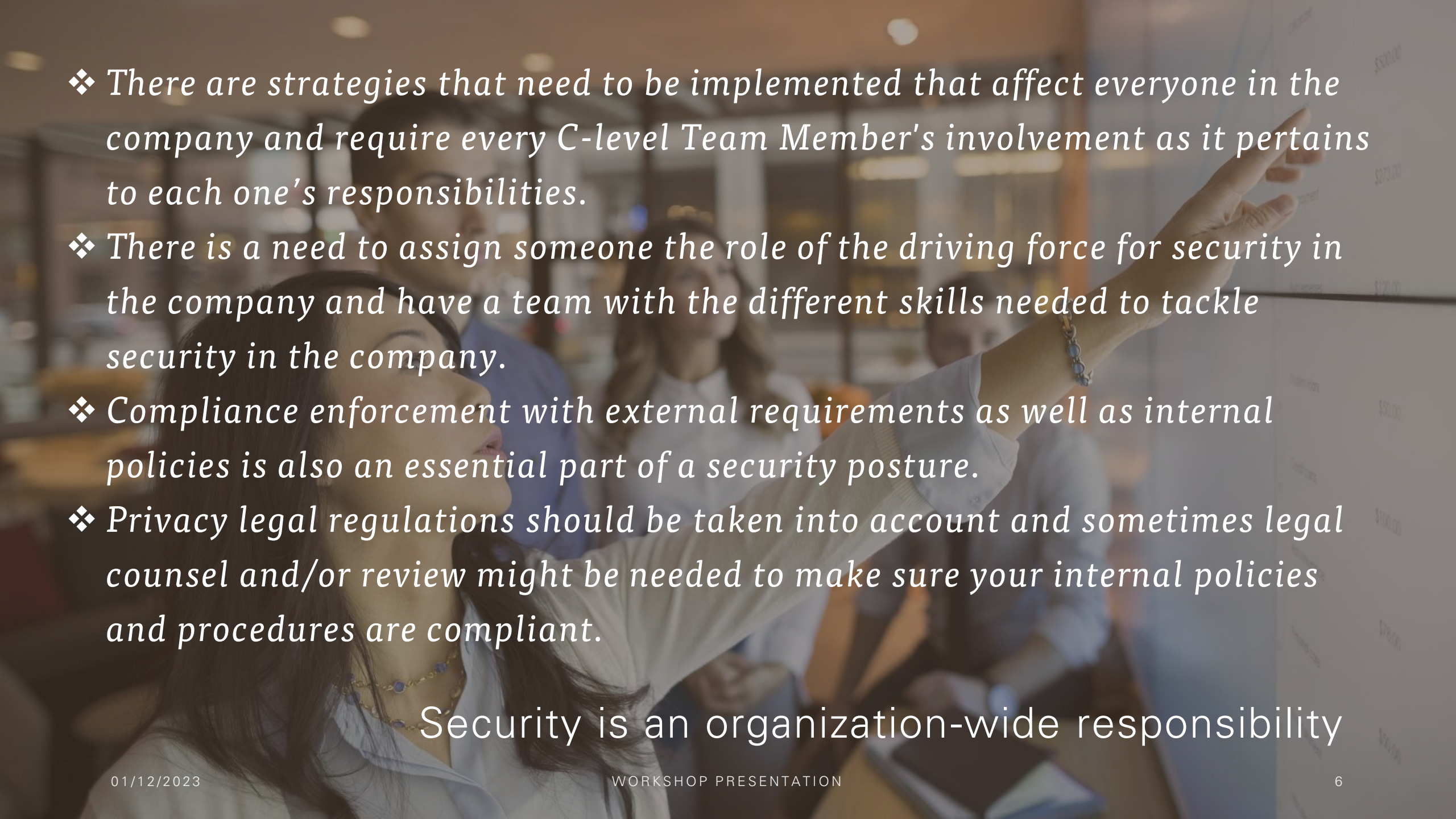
-The Latest 2022 Cyber Crime Statistics (updated December 2022) AAG, UK

Security Posture
Security Team

Identify your organization's most critical business processes and data to function.

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

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.



- *There are strategies that need to be implemented that affect everyone in the company and require every C-level Team Member's involvement as it pertains to each one's responsibilities.*
- *There is a need to assign someone the role of the driving force for security in the company and have a team with the different skills needed to tackle security in the company.*
- *Compliance enforcement with external requirements as well as internal policies is also an essential part of a security posture.*
- *Privacy legal regulations should be taken into account and sometimes legal counsel and/or review might be needed to make sure your internal policies and procedures are compliant.*

Security is an organization-wide responsibility

Strategic Planning to build a good security team

Every strategic plan starts with a Strengths, Weaknesses, Opportunities & Threats (SWOT) Analysis.

Skills Assessment

Internally, you must assess the skills within your current workforce to see how strong are they in security matters, both physical security and in cyberspace, and where is your organization weak

The Chief Information Security Officer (CISO)

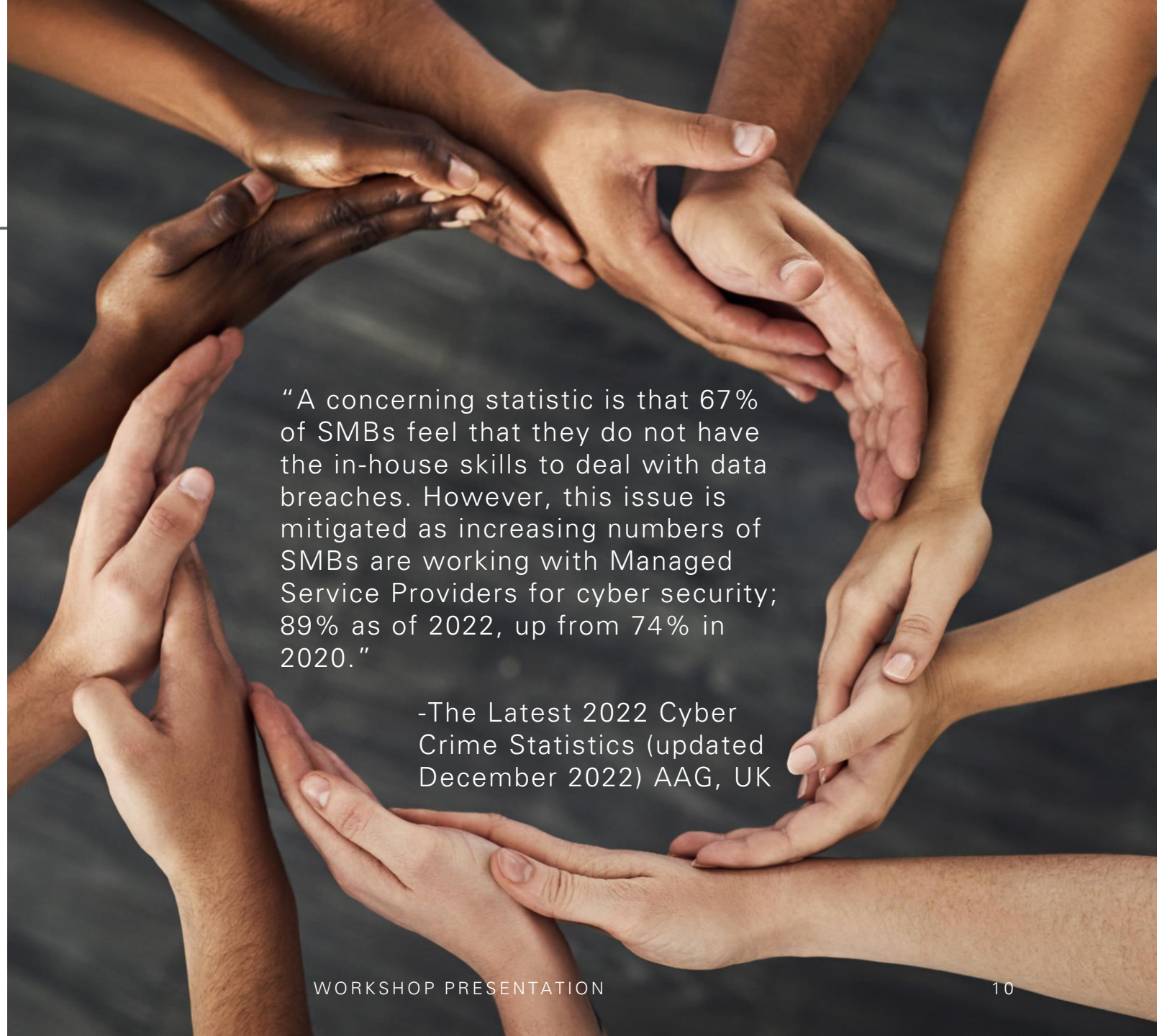
This SWOT analysis should be done with the assistance of a specialist in information security. If you are using a person in-house in your organization, this person should be with your C-Level Team.

The Chief Information Security Officer (CISO) is a position in organizations that has gained more relevance currently due to today's threats. It used to be a person reporting to the Chief Technology Officer (CTO) or Chief Information Officer (CIO), but today it is recommended to have this person at the C-Suite Level, on par with the CIO and/or CTO, since this person will focus on security only, overseeing not just the technical aspects of cybersecurity, but also the physical, administrative and human factors. As we discussed earlier, although this is the person with the role of driving security in the company, the issue is owned by the CEO, the Board of Directors, and all the C-Suite Team, including the CISO, as the implementation of the security strategies delineated by the organization touches every aspect of its operation.

Your current economic context

This SWOT analysis should include your current economic context measured against the existential risks your organization is facing.

The size of your operation and your economic context will be a deciding factor on the size and type of security team you need, whether it will be internal employees, external contractors, or a combination of both (usually a combination of both). Technology and service solutions can help you succeed in this area, even when dealing with limited resources.



SWOT Analysis

Strategic Planning to build a good security team

Physical access to client/business partner areas

If you receive clients/business partners in your physical facilities and you have other areas where you conduct operations for your organization that does not require their access, you need some type of physical access control to the protected areas with a register/log of visitors to those areas.

Physical Items

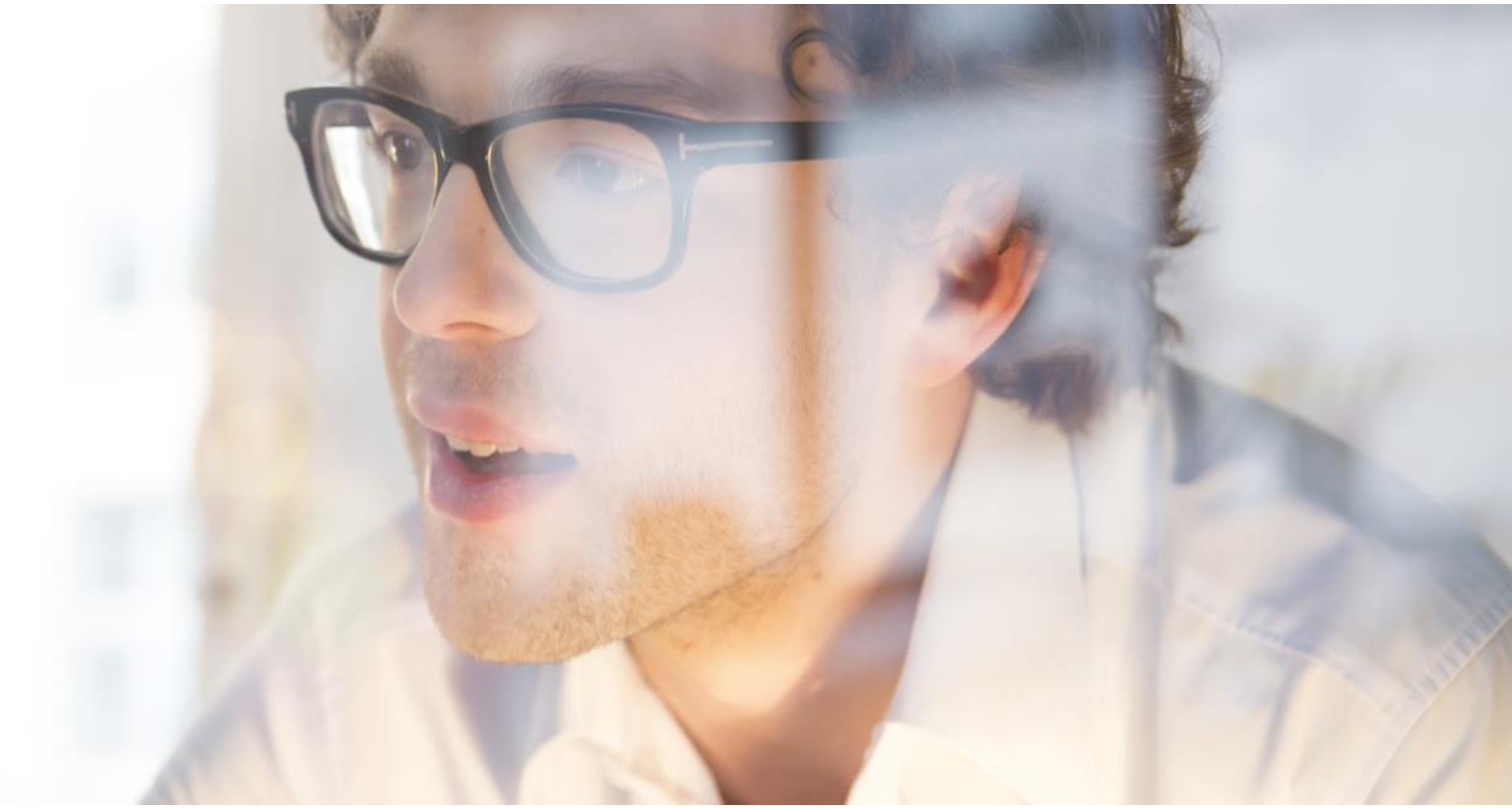
Handling of physical items (like documents, id cards, photocopies, photos, etc). A proper Chain of Custody procedure (that is, tracking and securing a physical item from when it is received to its disposal) might need to be implemented and audited to prevent the spill of information and attacks.

Governance, Risk, and Compliance

Internal policy-making to create the culture and values that will drive the organization in its security posture is necessary to mitigate business risks posed by security risks. Risks must be qualified and quantified/measured (using KRIs). The internal policies should align with any external compliance checklists like PCI DSS, the Risk Management Framework (RMF), and GDPR, which might involve data privacy issues. Policies need to be enforced for compliance. Auditing and non-compliance remediation actions and follow-ups are necessary for enforcing and being compliant. Planned strategies' progress should be measured (using KPIs).

Architecture

You need to analyze your current systems and process architecture to find any weaknesses and or space for improvement and to keep up to date with your business and security needs. The architecture needs to respond to your policies to support compliance. An experienced IT Engineer is usually a good alternative to help with this.



Data Loss Prevention

With the policies in place to protect data, there is a need to implement cyber measures to prevent the loss of the organization’s data in its systems. This is in addition to the Physical access and Chain of Custody measures above, as it
goes more to the hardware/software necessary for this function and the management of those tools.

Identity and Access Management.

Assess the current state of your identification, authorization, and permissions processes across all systems, both physical and in cyberspace. You might use a card access system to identify which personnel accesses which physical areas (open/pass through doors), have a CCTV system to monitor critical areas, and have a physical record and an electronic record of visitors who need to consent to video filming and maybe to a photograph for highly sensitive visits. You need to manage access permissions and access for employees/contractors to sensitive data.

Secure Devops / DevSecOps

The hands-on team that manages systems in the data center (or cloud) or at least manages security processes and functions securely need to be properly staffed (either internally or by a contractor). Analyze your current staffing to see if anything is needed here to ensure proper security posturing, as this team is responsible for securely installing, configuring, and operating systems and software, especially dedicated security products such as firewalls, intrusion detection, and even dedicated HSMs (Hardware Security Modules) to hold sensitive keys and certificates. Thus, they are responsible for applying security patches from suppliers in a timely manner to protect your organization from zero-day attacks.

Secure Software Developmen

If you develop any type of software in-house (even an automated Excel spreadsheet) your organization needs policies and procedures in place to do this in a secure manner. Applications have to be developed and tested to have minimal vulnerabilities. Application security testing can be done statically (code inspection) or dynamically (run-time behavior), but most organizations need to do both.

Supply Chain/Client Interconnections

Given the interconnected nature of today's supply chains, as one executive put it "The whole network is now at risk from the weakest link." As part of this evaluation, you need to assess the risk posed to your organization by your supply chain. Things like the merchandise you need to receive or send might be affected by an attack on your distribution supplier. Your systems might be compromised by a social engineering attack generated by one of your business partners' compromised systems. It just takes one compromised computer getting access to an email directory to spread an attack to hundreds of other organizations.

01/12/2023

Employee Training / Testing and the Organization's Security Culture

Train your employees constantly and test them more frequently to maintain awareness of the treats outside. Assess your current security culture. Are your employees security aware? Do they know when to identify a socially engineered phishing attack? Determine your vulnerabilities and create a strategy to minimize this attack surface on your employees, starting from the CEO.

Skill Background and Representation Diversity

A diverse cybersecurity team maximizes an organization's ability to bring innovation into its efforts and acts as a force multiplier for a company's capacity to combat digital threats," according to the 2020 The Business Value of a Diverse InfoSec Team report from the Institute of Critical Infrastructure Technology (ICIT), noting that leading CISOs see "diversity as both a competitive advantage and a solution to the growing talent shortage." Analyze the backgrounds of your team. It is good to have a representation of the population and different professional backgrounds on your security team. A person from a business background might see a threat that a person with a technical background might not. A person with a law enforcement background in security might have a different look into physical security.

Attack Identification Capabilities

Does your organization have any means of detecting an attack? How much time does it take for your organization to detect that it has been attacked? Seconds, minutes, hours, days, weeks, months, or years? Time to Identify an Attack is a measure of your organization’s security posture that can be compared to other organizations in your sector.

Forensic Analysis

It is necessary to have the technical skills available to make a forensic analysis to 1) determine if an attack has occurred, 2) determine the type of attack, 3) try to determine the source of the attack, and the attackers, 4) determine the extent of the attack and 5) collect evidence to be used in a trial when needed, following standard chain-of-evidence rules. Basically, this is detecting what an attacker did and how they did it. Analyze your current capabilities and needs.

Incident Response and Recovery

Once you detect an attack you need to respond to it. Once you have an initial forensics analysis, you can start the contention phase to try and minimize the danger to other processes, structures, and systems. Then you need to be able to repair the damage one and recover from the attack, hopefully in the fastest way minimizing damage. Also, here you need to have the continuity of operations plan to start executing by all involved parties, which could be all the organization in one role or another. Plans for communications, from the Board of Directors, employees, authorities, business partners, and the public, if necessary, should be executed with complete transparency and accountability. Time to Recover from an incident is a measure you can use to measure how well your response strategy works as compared to other organizations.

Penetration Testing

An important part of a security posture is to test your preparedness to prevent an attack. Penetration testing will tell you if the things you are doing to prevent an attack work. As part of this, you might be able to test your Forensic Analysis Skills, your Attack Detection Capabilities, and your Incident Response and Recovery capabilities. Also, from this, you will get recommendations on how to harden systems against future attacks. If you are not doing this, try to make up a strategy to take care of this.

Disaster Recovery Plan Execution Testing

You may have in place a backup system in a cloud to fire up if your main system is compromised or you might have some manual procedures to execute to keep operations running. Any system that you produce to try and keep your operations running during the effects of an attack, you must test it and update it regularly. You need to develop a policy on these tests and compliance with them should also be measured as part of your security posture.

Exercise

Make a preliminary SWOT analysis to start the process of creating a good security team.