CYBERSECURITY AND PROJECT MANAGEMENT

Event Recap
Greg Dubois

I summarized of the presentation which using A-I of the Alphabet:

A: Awareness - organizations and individuals must be strongly aware of the importance of Cyber Security for projects and as a standard part of doing business.

B: Backup - we must backup our files, but also we have to backup our systems

C: Community - our communities are great resources for information and knowledge including finding mentors outside of our organizations to provide new perspectives and to challenge our thinking

D: Defend - we must defend ourselves and organizations from cyber attacks. Use the Zero Trust method.

E: Education and Everyone - we must continuously increase our knowledge which can include obtaining certifications; and recognize that everyone is part of our cybersecurity system and in a sense, everyone is a cybersecurity project manager.

F: Financial Risk - our projects should include contingency for financial risk to our projects and money will need to be appropriated to address this.

G: Guidelines - guidelines must be established by the organization that address cybersecurity (SOPs, multi-factor authentication, etc.)

H: Hybrid - Most if not all of us work in a hybrid environment and use a combination of our cell phones, work computers, working from the office and from anywhere and there must be planning/contingency to address the hybrid work environment.

I: Innovation - we must think out of the box and be open to change and improving our ways of working and having contingency to address the zero day hack.

Europe - Turkey
Soner Çelik

Question:

What are the Major Challenges in Cybersecurity projects today? How Can you overcome them?

Answer:

As a project manager you are beginning to or have started to take more steps towards making sure your project and your personnel are cyber safe which is all very important. In my view here are some major challenges;

#1. Increase in Cyber attacks
Hackers are getting better at offense; companies aren't getting better at defense. The bad guys are getting worse faster. Every year, certain threats grow rapidly as cyber criminals focus their efforts on a particularly effective or lucrative attack technique, such as ransomware or cryptojacking. However, one of the most worrying trends in 2021 was the growth of cyber-crime across the board.

#2. Supply Chain Attacks Are on the Rise
A supply chain attack is a cyber-attack that seeks to damage an organization by targeting less secure elements in the supply chain. A supply chain attack can occur in any industry, from the financial sector, oil industry, to a government sector. A supply chain attack can happen in software or hardware. Cyber-criminals typically tamper with the manufacturing or distribution of a product by installing malware or hardware-based spying components.

Supply chain attacks rose to prominence in late 2020, grew through 2021, and are likely to continue to be a major threat in 2022. the most famous is likely the exploitation of the Log4j zero-day vulnerability. Log4j is a widely-used Apache logging library, and the zero-day vulnerability allowed an attacker who could control the contents of log messages or their parameters to achieve remote code execution.

#3. Cloud Services Are A Primary Target
With the pandemic-inspired shift to remote work came a rapid adoption of cloud-based infrastructure and services. Software as a Service (SaaS) solutions closed crucial gaps – such as the need for online meetings and file sharing – and cloud-based infrastructure was more accessible and easier to manage by a remote workforce.

Since the rapid shift to remote and the cloud in 2020, companies have had the opportunity to close many of the biggest security issues caused by a rapid transition with little or no advance planning. However, some cloud security gaps still remain, and cyber threat actors continue to work to outpace security personnel at taking advantage of the newly vital role that cloud computing holds in the modern business. The first thing with cyber security is project managers might think it's not necessarily so important because the project might not be that long. The reality is you know you are a target for many bad actors that are out there and particularly with the increase of remote workers. Now you're having to protect not only a network within the organization or within a confined space of the office you're also having to protect data that is all over the place.

As a project manager you know it's better to be proactive and try to keep things safe than to try to figure out what to do in the event of an incident.

Question:

How has the "hybrid" working mode changed the cybersecurity project workflow?

Answer:

The COVID-19 pandemic drove a dramatic shift in how projects was done. The rise of remote work made employees' computers – often personal devices – a company's first line of defense, and the surge in cloud adoption to support the remote workforce and meet digital transformation goals created new attack vectors for cyber threat actors. Another impact of the shift to remote work was the widespread adoption of Bring-Your-Own-Device (BYOD) policies. By allowing employees to work from personal devices, companies may have improved productivity and employee retention but also lost vital security visibility and the ability to respond to infections that threaten corporate systems and solutions.

North America
Saby Waraich

Question:

What are the Major Challenges in Cybersecurity projects today? How can you overcome them?

Answer:

Here are some major challenges:

1. Cybersecurity skills gap: The shortage of cybersecurity professionals means organizations are competing to hire and retain staff. There isn't enough human resource to cover physical security or policy implementation, to name just two of the aspects required in securing data. As a Cybersecurity PM you need those resources to get your projects accomplished.

2. Complex environments and operations: Digital transformation means some organizations may still be in the process of moving from legacy architecture to the cloud. Many have multi-cloud or hybrid cloud environments with services from more than one provider. This adds more complexity to your projects.

3. Evolving security threats: Cyber-criminals are continuously devising new ways to exploit vulnerabilities and remediation can be costly. This is also taking resources away from getting your other high priority projects completed.

Here are some ways you can overcome these challenges: Extend your cybersecurity team by building partnerships with 3rd party vendors and resources. They can augment your staff with a pool of experts who as an extension of your team — collaborating in an agile, sprint-based model to defend against cyber-attacks.

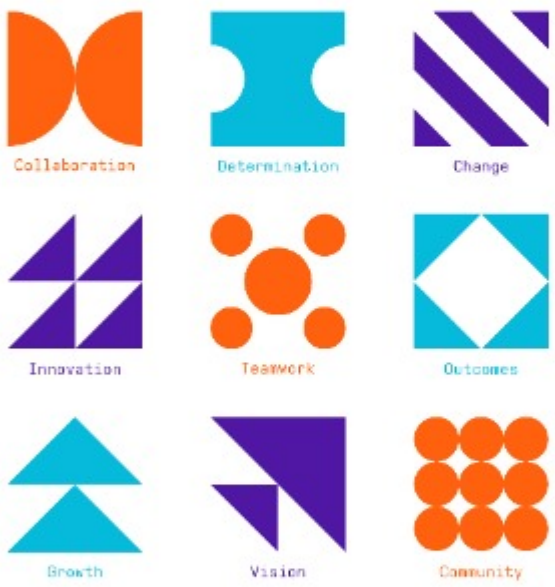
As your consistent support team, they have a deep knowledge of your environment and business operations to help you continually improve your security posture. Threat intelligence, security analytics, alerts and incident response services can be consolidated into a solution to be deployed and managed across your multi-cloud environments. You also need to plan for contingency for zero day trust attacks and add that as part of your project plan. Have risk response strategies documented.

Question:

How has the "hybrid" working mode changed the cybersecurity project workflow?

Answer:

During the pandemic, a new concept known as hybrid working was introduced in order to keep companies running. This concept of the hybrid workforce incorporates both work from home and office-based work. The change brought surprising yet positive results leading to enhanced performance and as a result, it quickly gained popularity among the companies and employees alike. However, with freedom comes responsibility and due to the hybrid situation, companies need to be much more vigilant regarding their security.



Asia

Md Showkat Ali

Question:

What are the Major Challenges in Cybersecurity projects today? How can you overcome them?

Answer:

Understanding the visualization and benefit realization by the stakeholders from the cybersecurity projects in overall Objectives of the organizations is a big Challenge. Still most people have a tendency to view cyber security as a pain corner and not a value adding item. Also the specific skills and experience required for the projects is another challenge.

To overcome those, the clear communication, clarity and proper awareness among all the stakeholders is the key. If everyone understands what is the value of the Cyber Security projects or risks on the overall organizational landscape, the support will be better and smooth. For the skills, proper resource recruitment, allocation and most importantly continuous knowledge upgrade through training, certification besides on job learning is a must.

Question:

How has the "hybrid" working mode changed the cybersecurity project workflow?

Answer:

Hybrid working mode is now very common across the globe which was mostly started in many places after the pandemic. It definitely has some benefits on Cybersecurity projects workflow as you can get easy reachability/arrangements with the needed stakeholders. The stakeholders have now less time spent on roads/traffic jams, more time with family which ultimately are adding value to the projects.

On the other hand, there are new risks involved due to this new mode. As the attack surface has increased now, the hackers have more options to get access to your valuable project data. Even the chances of exposure to physical risks like dumpster diving, shoulder surfing is also high. Proper take care of these risks like encryption in end to end communication path, usage of vpn and more awareness on related risks should not be overlooked to ensure successful cybersecurity project management in hybrid mode.

Latin America

Daniel Abellá

Question:

What are the Major Challenges in Cybersecurity projects today? How can you overcome them?

Answer:

Cybersecurity must be top of mind for all project managers--regardless of the nature of the projects they are working on. The main challenges are an increase in the overall number and sophistication of cyber-attacks. We also have expanded our online collaboration and data exchange between teams and vendors, which expose us to be victims of cyber-crime around the clock.

There are few thing we should always do to overcome these challenges. First, make cybersecurity part of both, our project charter and risk register, which translates in an active management of cyber as a risk category in every project. Every project team should have a cybersecurity SME to assist in these processes.

Next, adopt a sound cyber policy that includes at least the most basic practices like always up-to-date systems and credential hygiene (use of multi factor authentication or password-less technologies to access critical systems and data are very helpful.)

It's specially important to enforce this type of policy and controls through the supply chain of your project, as one inept vendor with an un-patched operating system or a compromised password is all it takes to be victims of a cyber attack.

Question:

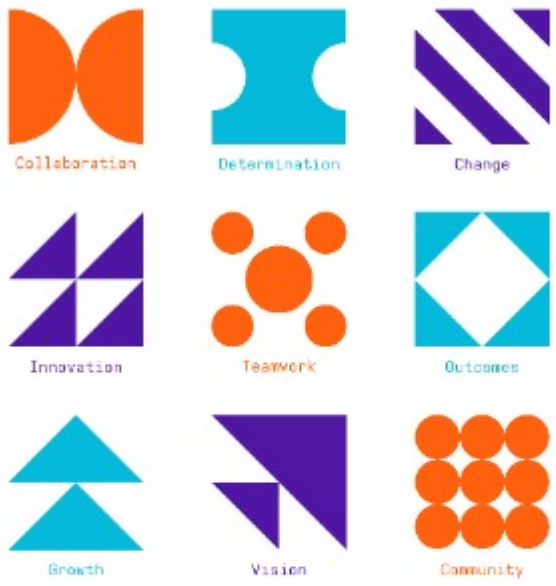
How has the "hybrid" working mode changed the cybersecurity project workflow?

Answer:

Technology allowed us to continue working and achieving our objectives from virtually anywhere. The other side of this coin is that it expanded the attack. Before, most critical data resided on our company or customer premises. Today, this data is being shared and can be accessed via different devices from diverse locations.

In this type of scenario, it is imperative to assume compromise and have mitigation plans in place. We should be proactive in protecting assets and identities, detect when something out of the ordinary happens, and should an incident occur, have a plan on how to respond.

Today, these controls, mitigations, and contingencies need to be constructed, with help of SME's, during project planning and monitored through the project as with any other high priority risk.



Africa

Barbara Chinzunza

Question:

What are the Major Challenges in Cybersecurity projects today? How can you overcome them?

Answer:

Cybersecurity is a fairly young and fast growing industry; the lack of maturity brings in a lot of uncertainty to cybersecurity related projects. In light of this , the project management function will need to work closely with the cybersecurity subject matter experts to ensure that the project goes through a thorough risk management process. Failure to identify the risks will result in insufficient implementation of security controls leading to security breaches.

Globally, most organization are still hesitant to provide a budget for Cybersecurity projects and only do so when they have suffered a cyber attack. To overcome this shortfall, the project management office should construct a business case that clearly articulates the financial and non-financial benefits that accrue as a result of the project implementation. This will help the project steerco to fully support the project and also communicate to everyone in the organization to understand their role towards implementation of a secure environment.

Question:

How has the "hybrid" working mode changed the cybersecurity project workflow?

Answer:

A hybrid team consists of a workforce that is working from multiple locations across the globe. COVID19 and also technological advancement accelerated the adoption of the hybrid working mode.

The challenges in a hybrid team are much more complex because project managers have to handle employees from different departments, remote locations and cultures. Some of the challenges include communication gaps, inaccurate scheduling, poor collaboration and lack of real-time updates on the project metrics. In light of these challenges automated project workflow tools such as "Project Manager" and "Basecamp" have been adopted to ensure that the project remains on schedule and productive. Frequent meetings are also critical for better communication and collaboration.

This Insight Xchange Nugget
is powered by volunteers across the world:

Priya Patra
PMI Mumbai

Pedro Branco
PMI Sao Paolo, Brazil

Arief Prasetyo
PMI Indonesia

Dhammike Mendis
PMI Colombo, Sri Lanka

Collaboration

Yudha Pratama
PMI Puget Sound

CHAPTER EXCHANGE

A PMI CHAPTERS COLLABORATION

Have a suggestion?

Feel free to drop a note to the PMI Chapter Xchange team by sending email to:
pmichapterxchange@gmail.com