Trinidad And Tobago
Cyber Security
Incident Response Team

Incident Response, Resilience and Digital Transformation in Caribbean Credit Union

Mr. Angus Smith
Manager – TTCSIRT

The World Today

The COVID 19 Pandemic - Agent of change

- *Increased online activities - browsing, commerce, application for aid*
- *Work from home – Remote access*
- *Increased Online commerce – Shopping and Banking*
- *Online Vaccine Appointments - Web or Social Media*

Increase Digital Transformation projects

- *The move from manual processing to online or electronic/digital systems for operational activities to facilitate online access by staff and customers*

Results of this new way of doing business

The organization can be impacted by cyber security threats which can affect the day to day operations of the organization increasing the risk surface of the organization.


HACKER
SPAM
WORM
WORM
SPAM
SPAM
VIRUS
WORM
HACKER

Cyber Security Threats to Credit Unions

- *Malware – Ransomware and Phishing Attacks - Bitcoin, Data Disclosure*
- *Denial of Service*
- *ATM Skimming*
- *Pandemic Themed Attacks – use of COVID 19 to solicit personal information*
- *Supply Chain Attacks – through partners, vendors, suppliers*
- *Fraudulent Wire payments – Business email compromise*
- *Card not present fraud - a result of the move to EVM CHIPS*
- *Unauthorized access to online financial accounts – money transfer*
- *Use of Social Media to impersonate company's Facebook , twitter, Instagram*

Reasons for Cyber breaches

People	Lack of Cyber Hygiene practices Lack of a Cyber Security Awareness Program Lack of trained staff or staff assigned to the task of responding cyber security issues
Process	Lack of a Risk Management approach for Cyber Security Risks Lack of cyber security policy, information security policy and BCP\DR policy. Lack of incident response policy – who to inform when an incident occurs
Technology	Inadequate or non-existent updates and patches management Misconfigured Hardware Devices (firewalls, network devices servers, desktops) Misconfigured software (Server and Desktop OS, VPN, Web Applications, Websites

Cyber attacks

BECU in Tukwila Washington (26b assets 1.28 mil members)

- *One credit union customers affected by attackers using scams to target customers asking for personal information to help provide payments .*
- *The acquisition of member information on the black market using it to attempt to break into member accounts.*

SOLARWINDS

Attack on supply chain which put financial institutions on alert.

ANSA MCAL / TATIL

- *Ransomware attacks with information posted on the Dark Web.*

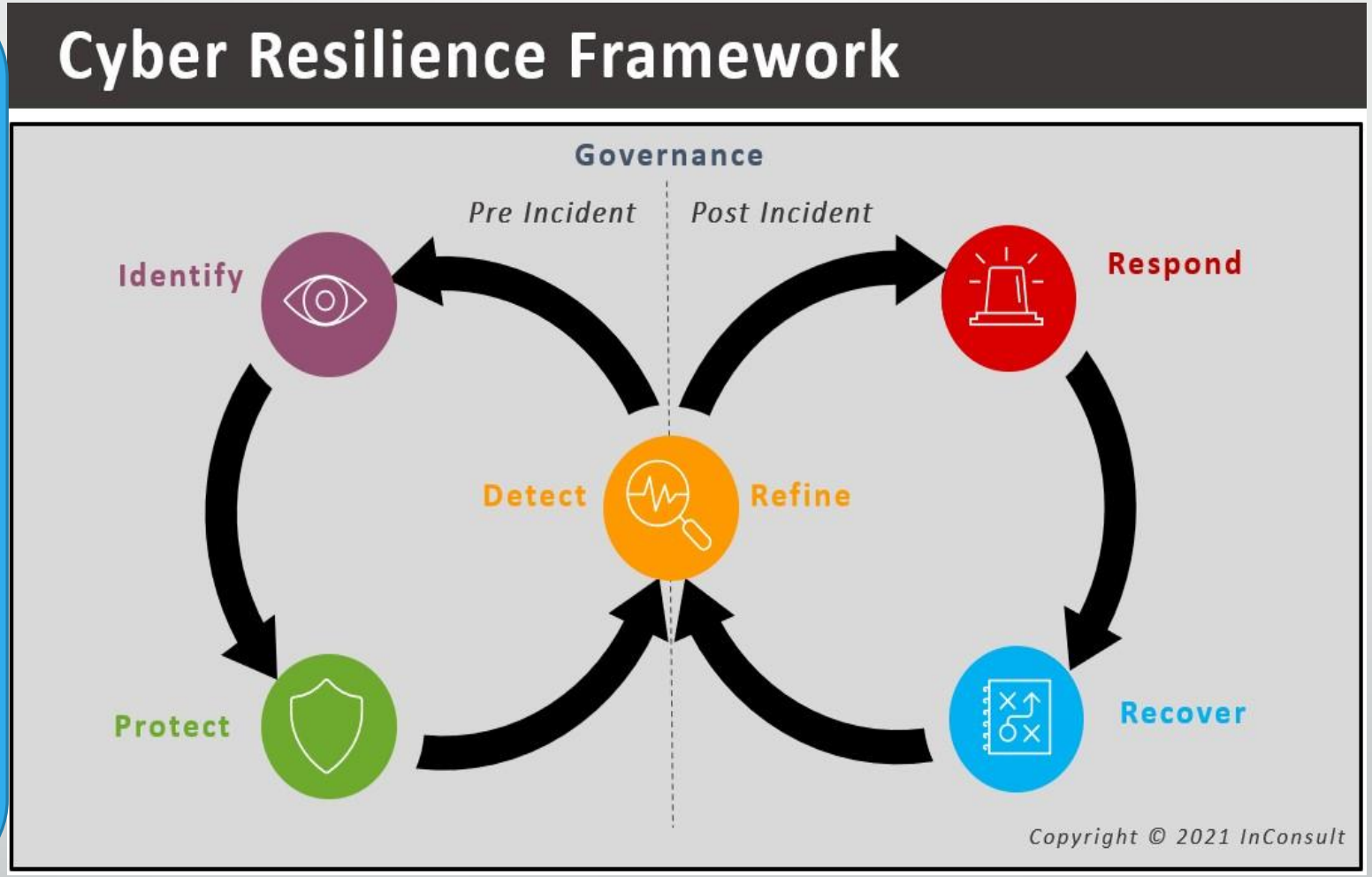
LOCAL

- *Social media cloning scams – impersonating Facebook pages to retrieve account information*


Cyber
Resilience

Resilience through a Cyber Security Framework

Cyber resilience is the measure of an organisation's ability to continue with working as normal while it attempts to prevent, detect, control and recover from threats against its data and IT infrastructure



Cyber Resilience Framework

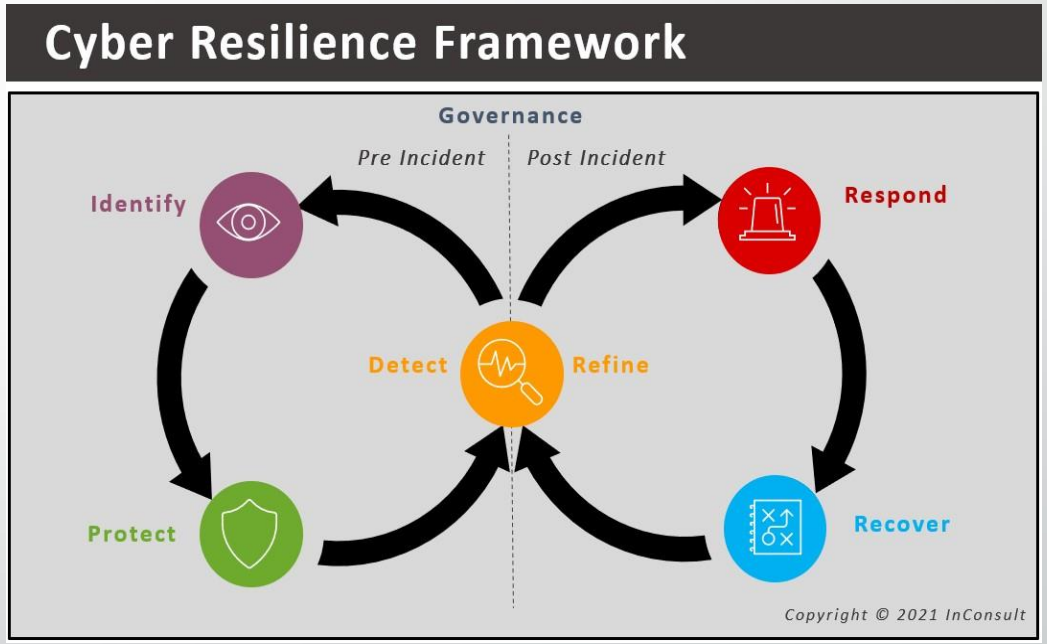
Identify critical assets, systems and data. The enterprise must understand the resources that support all critical functions within a business context

Protect critical infrastructure services. In this step, the enterprise installs first-line security programs that will limit or contain the impact of any potential threat.

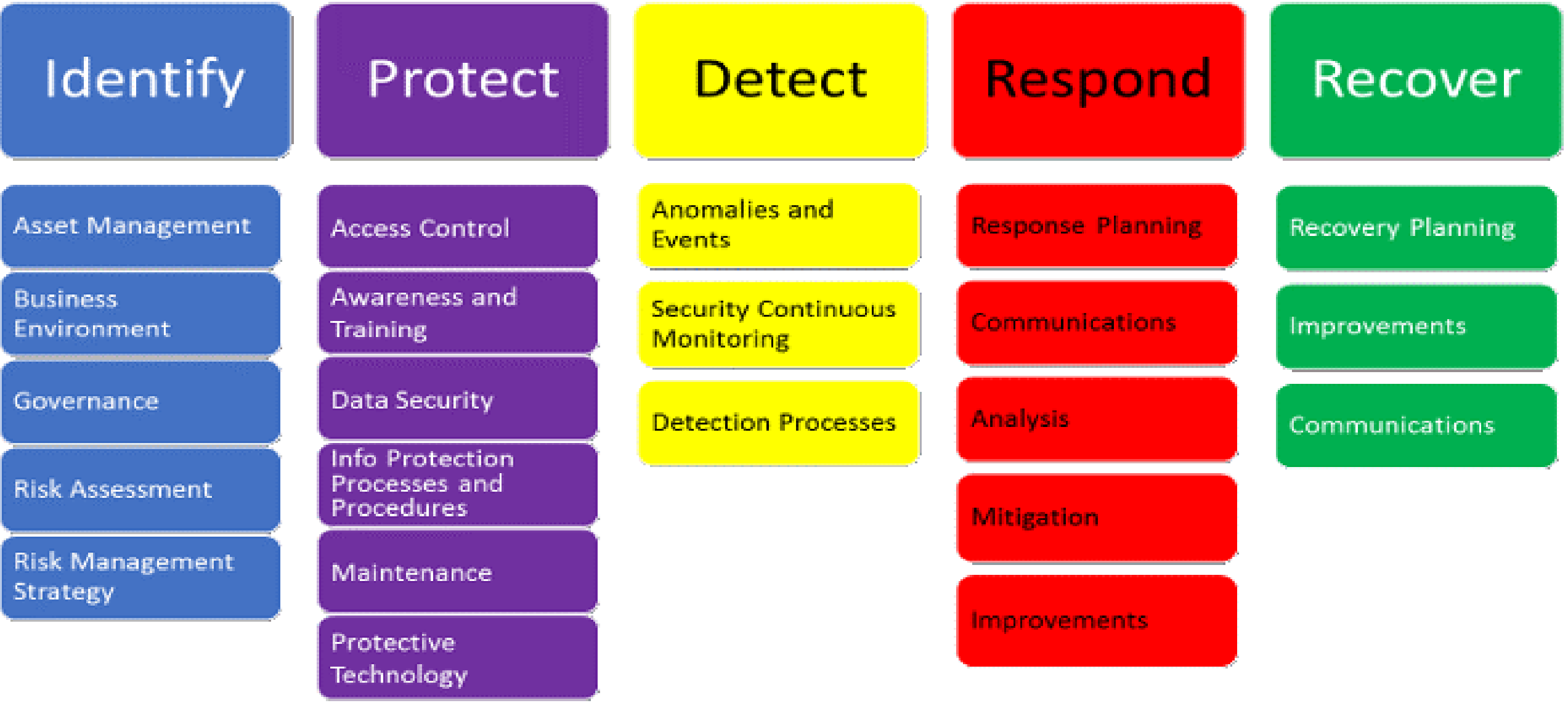
Detect strange events and suspected data breaches or data leaks before major damage occurs. This step demands constant security monitoring.

Respond to a detected security breach or failure. This function involves an end-to-end incident response plan to ensure business runs as usual in the face of a cyberattack.

Recover to restore any affected infrastructure, capabilities or services that were compromised during a cybersecurity incident. This step focuses on making a timely return to normal efforts.



NIST Cyber Security Framework



Strengthen your Cyber Resilience Framework

Assign Incident Response to Senior Resource

Assign a senior resource and your organisation will have someone to champion cybersecurity at the C-suite level. Management must be invested in the development of a Cyber Security program in the organisation. They will help educate board members and garner their support for investment in incident response automation tools and developing a comprehensive cyber resilience framework

Develop a culture of Cyber Resilience

Organisations must educate the first line of defence by encouraging *the entire workforce* to adopt a mindset of cyber resilience. All employees should know how to identify and detect malware and phishing threats, and they should understand the results of a cyber attack. Leaders must promote teamwork, open communication and sharing across teams. Through peer learning and ongoing education, an organisation can instil a security-focused culture that serves as a solid foundation for the cyber resilience framework

Develop formal Cybersecurity Policies

A good risk management policy is an integral aspect of a cybersecurity framework. When your organization has documented proven security processes as part of their official guidelines, your employees have a reliable set of protocols to guide their efforts. A risk management policy should be data-driven, which enlists your IT security team's skills to identify critical assets and advise on how best to protect them. Incident Response Plan and Asset Management Plans should be a must

Cyber Resilience at the Board Meeting

Keep in mind your incident-response strategy and overarching cyber resilience framework are dynamic, evolving assets. They are not one-and-done tasks .It's crucial that you review your policies and security practices. A robust security posture is not possible if all security issues are not shared with key stakeholders, communication is key. Leaders must check in with key stakeholders on security policies. In doing so, your business can maintain a high level of cyber resilience, so the organization is prepared to respond and manage any threats

Train your operational staff

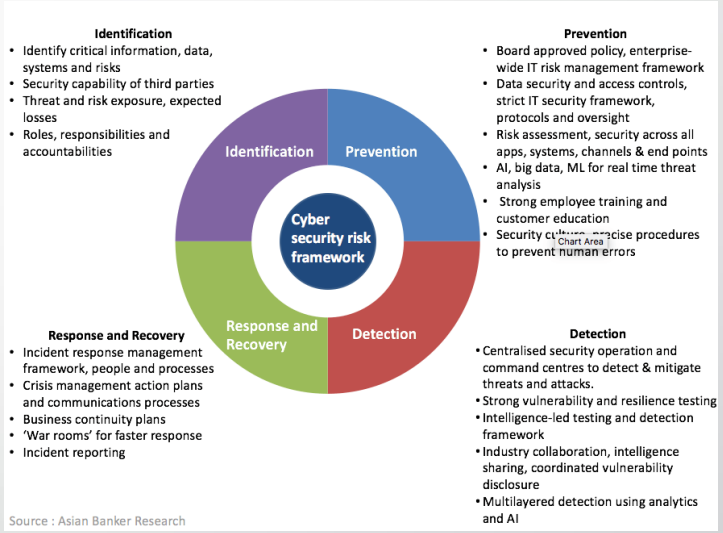
The best security professionals want opportunities for continuous learning and career growth. If they don't see viable ladders up in their job, they will move to another one. By growing talent within the company with ongoing training, you keep your staff engaged. In return for offering a platform that facilitates personal and professional growth, you cultivate a loyal workforce of highly-skilled security professionals

Cyber Resilience in the organisation

The key to building cyber resilience is to focus less on technology and more on people. You can only leverage power of data and leverage the latest technology tools when you have a skilled team in place to oversee your security operations.

Cyber resilience should not be left to the security team alone. Instead, C-suite members must work hard to establish a strong culture that promotes peer learning, open discussion, and ongoing training on the latest incident response tools and cyber resilience strategies.

Integrating a holistic approach that takes all people and processes of the organisation into account, your cybersecurity framework will be a constantly-evolving element of the organisation's operations.




INCIDENT
RESPONSE

Developing your Incident Response

Establish a formal incident response capability

Even if your organization is small, take incident response seriously and establish a formal incident response body. Even if it is a virtual incident response team with part-time staff, defining this team and giving it authority and responsibility will dramatically improve your capability to respond when a cyberattack strikes.

Create an incident response policy

The guidelines from which the incident response plan is developed, it lays out the organizational framework for incident response. It specifies what is considered a security incident, who is responsible for incident response, roles and responsibilities, documentation and reporting requirements.

Define an incident response plan

An incident response plan isn't just a list of steps to perform when an incident happens. It is a roadmap for the organization's incident response program, including short- and long-term goals, metrics for measuring success, training and job requirements for incident response roles.

Develop incident response procedures

The detailed steps incident response person/teams will use to respond to an incident. They should be based on the incident response policy and plan and should address all four phases of the incident response lifecycle

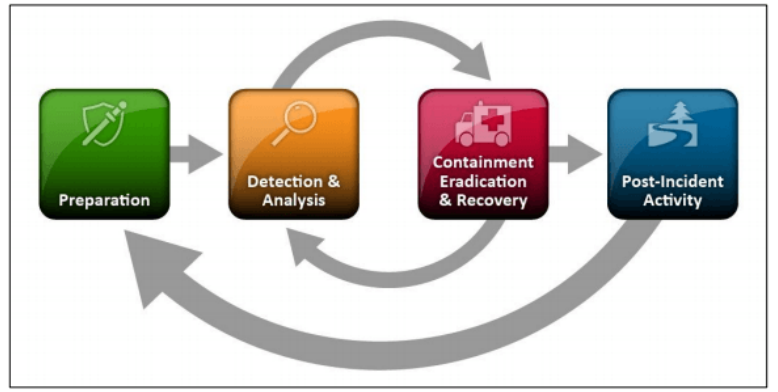
Incident Response Lifecycle

Preparation: In order prepare for incidents, compile a list of IT assets such as networks, servers and endpoints, identifying their importance and which ones are critical or hold sensitive data. Set up monitoring so you have a baseline of normal activity. Determine which types of security events should be investigated, and create detailed response steps for common types of incidents.

Detection: is the collecting data from IT systems, security tools, publicly available information and people inside and outside the organization, and identifying precursors (signs that an incident may happen in the future) and indicators (data showing that an attack has happened or is happening now)

.

Analysis involves identifying a baseline or normal activity for the affected systems, correlating related events and seeing if and how they deviate from normal behavior.



Post-Incident Activity

- What happened, and at what times?
- How well did the incident response team deal with the incident? Were processes followed, and were they sufficient?
- What information was needed sooner?
- Were any wrong actions taken that caused damage or inhibited recovery?
- What could staff do different next time if the same incident occurred?
- Could staff have shared information better with other organizations or other departments?
- Have we learned ways to prevent similar incidents in the future?
- Have we discovered new precursors or indicators of similar incidents to watch for in the future?
- What additional tools or resources are needed to help prevent or mitigate similar incidents?

Restoration of services in the quickest timeframe.

Resiliency

Containment : is meant to stop the attack before it overwhelms resources or causes damage. A containment strategy will depend on the level of damage the incident can cause, the need to keep critical services available to employees and customers, and the duration of the solution—a temporary solution for a few hours, days or weeks, or a permanent solution.

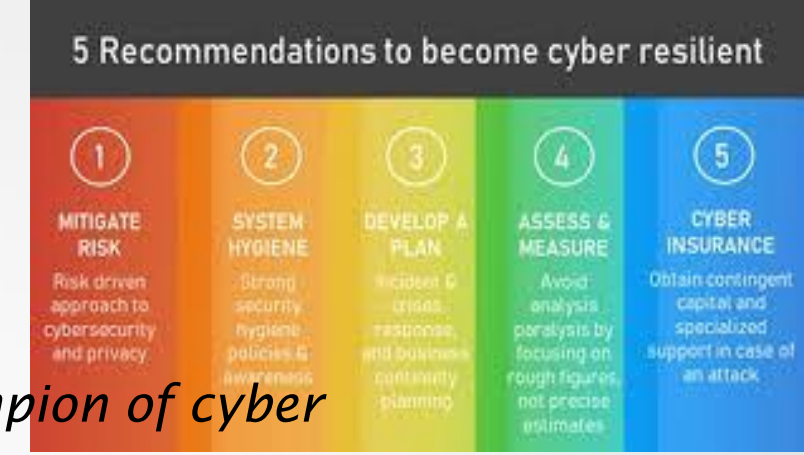
As part of containment, it is important to identify the attacking host and validate its IP address. This allows you to block communication from the attacker and also identify the threat actor, to understand their mode of operation, search for and block other communication channels they may be using.

Eradication and Recovery: after the incident has been successfully contained, you should act to remove all elements of the incident from the environment. It can include identifying all affected hosts, removing malware, and resetting passwords for breached user accounts. When the threat is eradicated, restore systems and recover normal operations as quickly as possible, taking steps to ensure the same assets are not attacked again.

Measures to assist in incident recovery

- Backups of Data
  - Tested and verified
  - Hot or cold backups
  - Full and incremental
- Redundant network connections (internet, LAN and WAN connections)
- Redundant Hardware.
- List of Vendor contacts.
- SLA Agreement for critical software and hardware.
- Documented network configurations and administration passwords.

Key Points to Note



- *Assign someone at C-Level to be in charge and be a champion of cyber security.*
- *Identify cyber risks to the organisation by adopting cyber risk planning.*
- *Develop and implement an Incident Response Plan.*
- *Assign a resource to be the focal point of the plan – Main responder/s or a Point of Contact.*
- *Educate your employees and develop a Culture of Cyber Hygiene.*
- *Identify external resources to assist in the recovery from an incident -vendors or local CSIRT.*
- *Maintain hardware and software with required updates*
- *Ensure security staff subscribe to resources which provide information on latest threats (CSIRT/CERT, Industry Sources)*
- *Approach Cyber Security Resilience as a Team with everyone being responsible*

Trinidad And Tobago
Cyber Security
Incident Response Team

Stay Connected!

@TTCSIRT

SIGN UP FOR OUR MAILING LIST AT HTTPS://TTCSIRT.GOV.TT