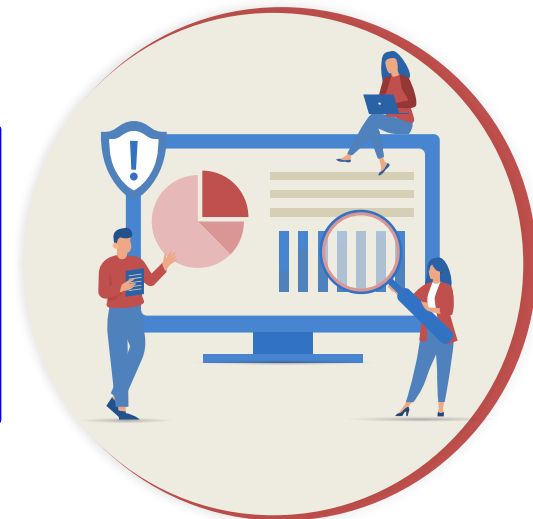


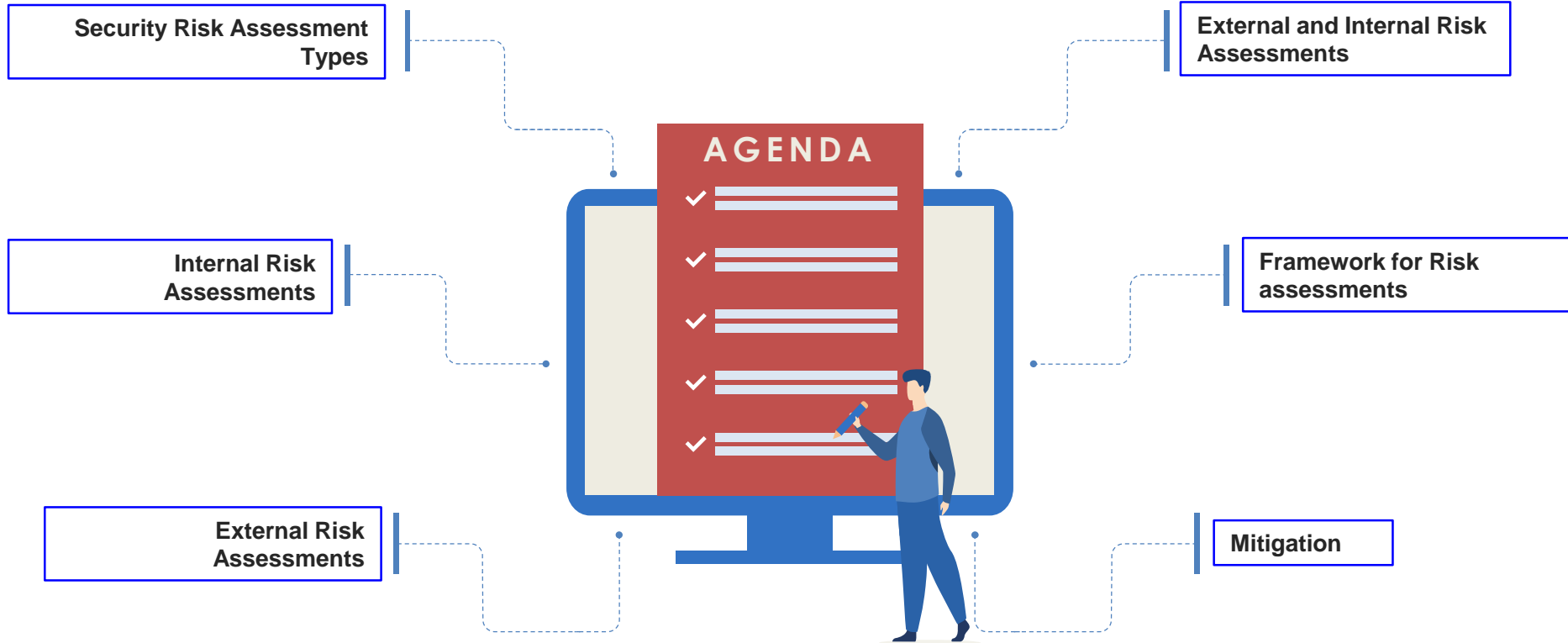
Security Risk Assessment Types



Milton Kabia
ISSO/IT Security Director
ANTHC



Agenda



Security Risk Assessment Types

Many Types

- Facility physical vulnerability
- Information systems vulnerability
- Physical Security for IT
- Insider threat
- Workplace violence threat
- Proprietary information risk
- Board level risk concerns
- Critical process vulnerabilities
- Brand risk
- Reputation risk

MAIN TYPES

Internal
External
Internal + External

Approaches

Self-directed Assessment: Use only internal resources

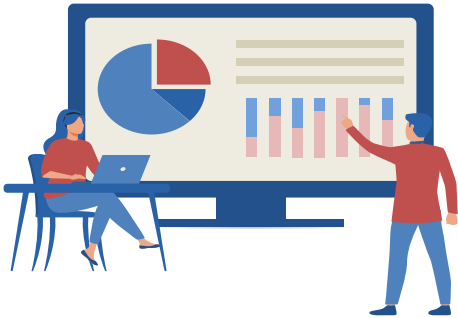
Collaborative Assessment: A combination of internal and external resources

SWAT Team Assessment: Performed quickly and thoroughly by external resources

Red Team Assessment: An independent group seeks to challenge an organization to improve effectiveness, utilizing highly experienced personnel with a specific scope and objectives

Internal Risk Assessment

01



Perform by Internal IT Security Team

- Hardware Assets
- Wireless
- VLANS
- Networking
- Firewall

Mostly involve vulnerability Assessment

External Risk Assessments

02



Perform by external agencies such as:

- CISA
- DHS
- Hired Contractors

Assessments may involve:

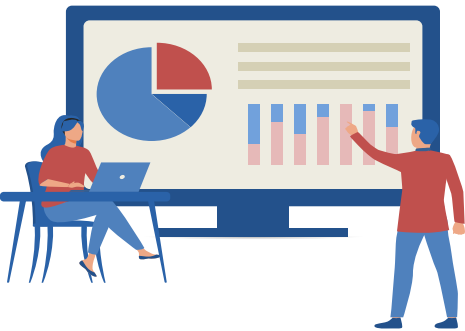
Evaluation of:

- Governance documents – Policies
- People, process, and technology

Vulnerability assessments & Penetration testing

Internal & External Risk Assessments

03



Perform by Internal IT Security Team & external agencies such as:

- CISA
- DHS
- Hired Contractors

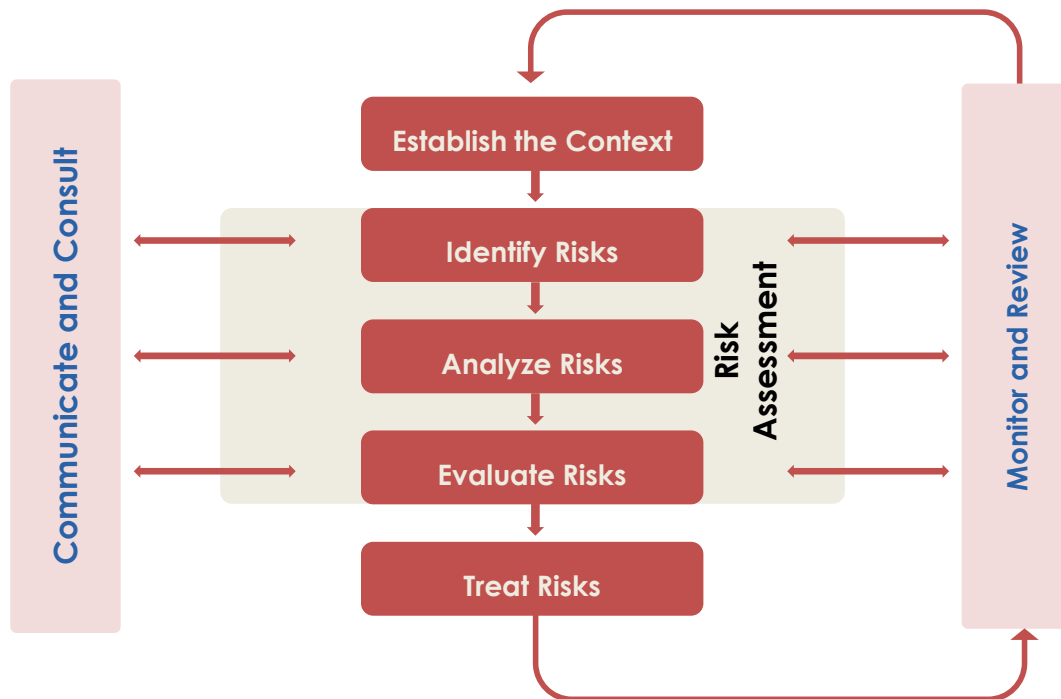
Assessments may involve:

Evaluation of:

- Governance documents – Policies
- People, process, and technology

Vulnerability assessments & Penetration testing

Framework for Information Security Risk Management



Information security risk management should be a continual process that contributes to

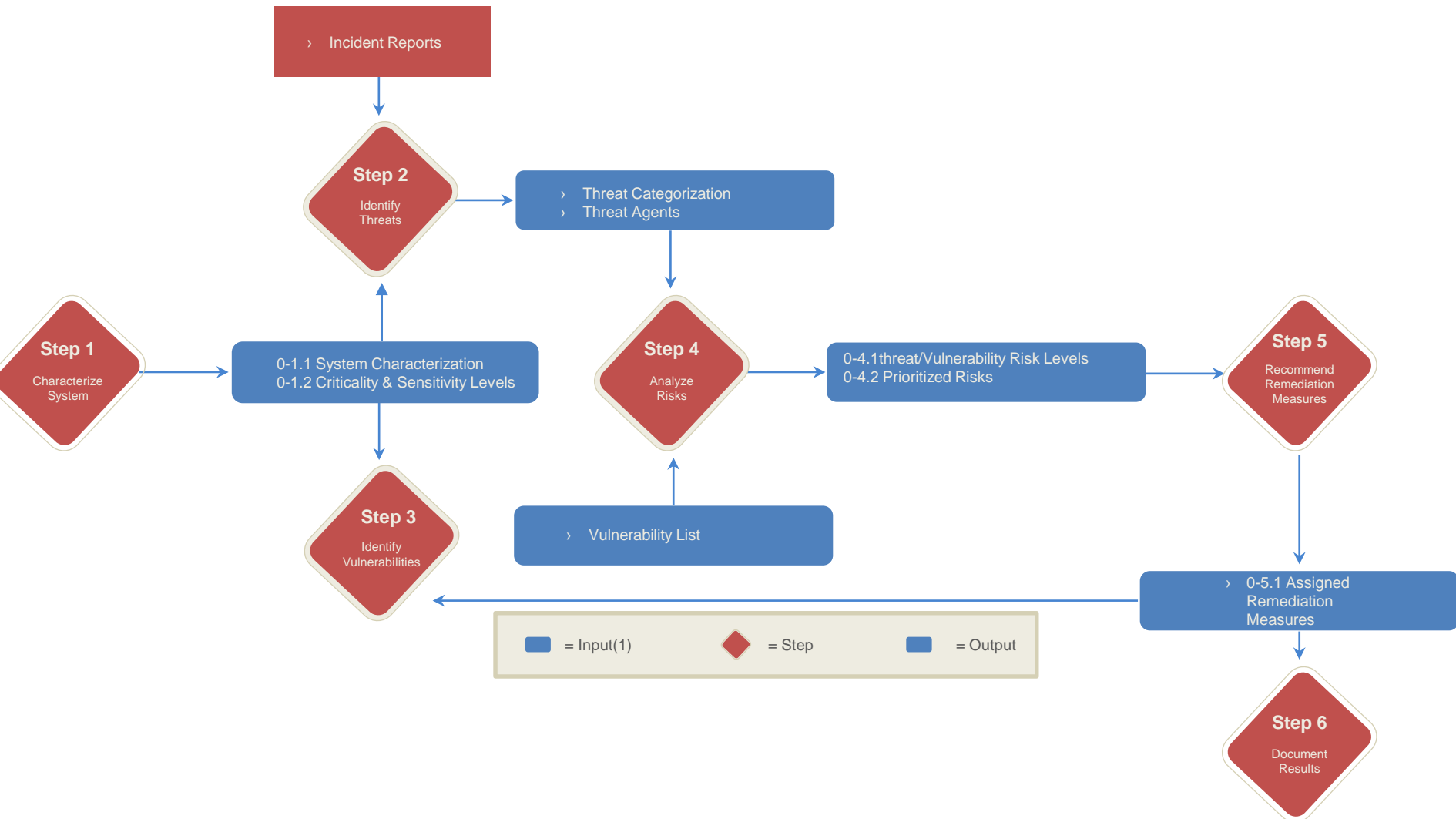


- 01 Identifying and assessing risk
- 02 Understanding risk likelihood and the consequences for the business
- 03 Establishing a priority order for risk treatment
- 04 Stakeholder involvement in risk management decisions
- 05 The effectiveness of risk treatment monitoring
- 06 Staff awareness of risks and the actions being taken to mitigate them

Gap Assessment of Organization Information Security



Introducing Information Security Risk Assessment Process Workflow



Process for Information Security Risk Assessment



Identifying internal and external information security threats

- › Internal threat : Employee data leak
- › External threat : Malware & Phishing
- › Lack of governance documents
- › Lack of Security Awareness and Training

01

02

Allocating vulnerability rating to different information assets

- › 0-2.9 : Low severity
- › 3.0 – 5.0 Medium severity
- › 5.1 – 6.0 High severity
- › 6.1-9.9 : Highest severity

Assessing level of risk associated with different class of asset

- › 1 : Low risk level – Assets?
- › 2 : Medium risk level
- › 3 : High risk level
- › 4: Very High risk Level

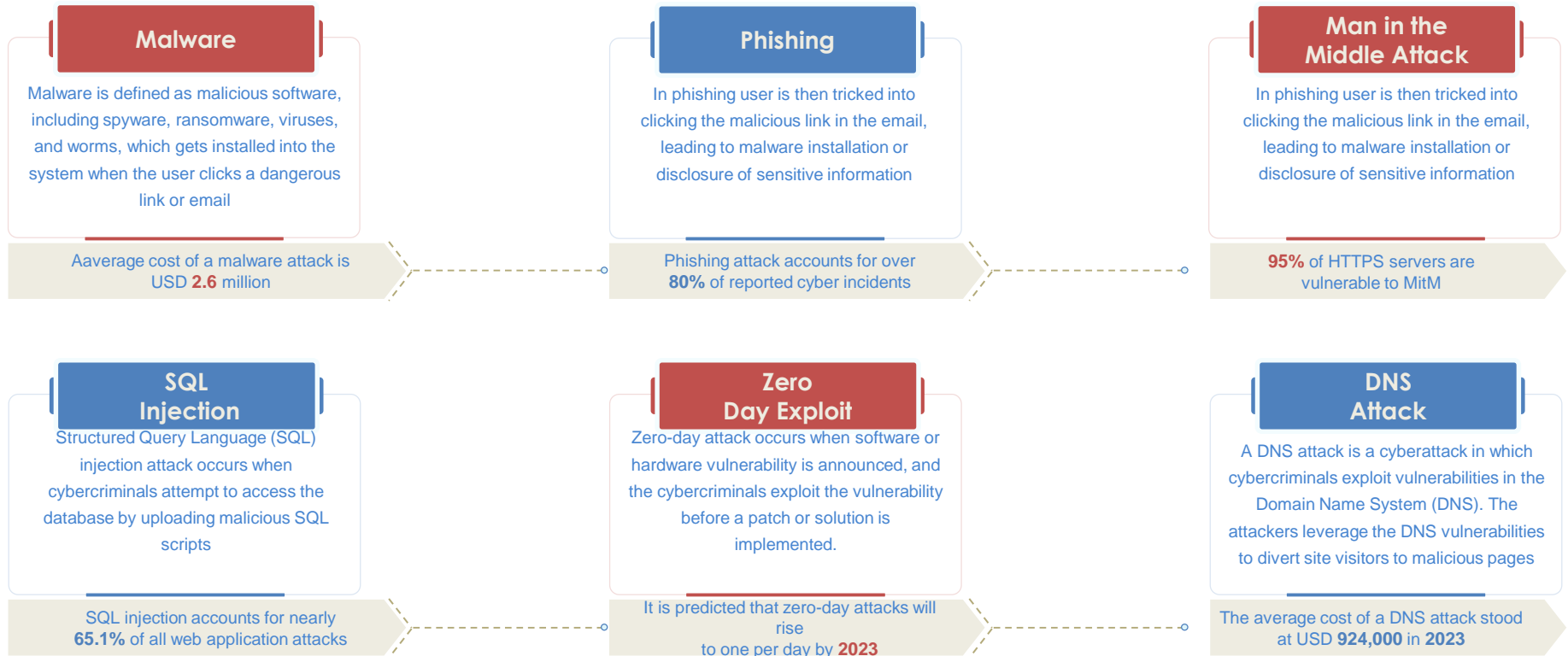
03

04

Identifying level of risk on the basis of vulnerability level and threat

- › Financial
- › Reputational
- › Regulatory

Information Security Attacks Faced by Organization








KPIs to Measure Information Security Risk Management

KPIs	Description	Before Information security risk management programme	After Information security risk management programme
○ Intrusion Attempts	Number of times attackers tried to breach into network of organization	32	18
○ Mean Time Between Failures	Time exists between system failures when looking to determine reliability	2 days	1 day
○ Non-human Traffic	Amount of traffic indicating potential cyber attack from bot	245 users	98 users
○ Mean Time to Resolve	Time taken by employees to respond after identification of threat	1 day	3 hours
○ Days to patch	Time taken by employees to implement security patches	5 days	3 days
○ Cost per incident	Cost incurred to respond and resolve an attack	\$5,000	\$3,400

Risk Assessment Matrix with Vulnerability and Threat Level

Risk Assessment Matrix		Vulnerability Level				
		Very High	High	Moderate	Low	Very Low
Threat Level	Very High	Very High	Very High	High	High	Moderate
	High	Very High	High	Moderate	Moderate	Low
	Moderate	High	Moderate	Moderate	Moderate	Low
	Low	High	Moderate	Moderate	Low	Very Low
	Very Low	Moderate	Low	Low	Very Low	Very Low

 Very High Risk	 High Risk	 Moderate Risk	 Low Risk	 Very Low Risk
---	---	---	--	---

Identifying Information Security Threats and Impact on Organization



Threats

01 >>>

Errors and Omissions

- > Intentional mistake by employee
- > Accidental mistakes in manual programming

■ High

02 >>>

Fraud and Theft

- > Theft by internal employee
- > Fraud in financial system by insider

■ Low

03 >>>

Employee Sabotage

- > Destroying hardware of facilities
- > Holding data hostage

■ High

04 >>>

Physical Infrastructure Loss

- > Loss due to earthquake
- > Loss in information due to flood and fire

■ High

05 >>>

Malware

- > Computer viruses
- > Trojan horses and worms

■ Low

Examples

Impact on organization

Examples	Impact on organization
<ul style="list-style-type: none"> > Intentional mistake by employee > Accidental mistakes in manual programming 	■ High
<ul style="list-style-type: none"> > Theft by internal employee > Fraud in financial system by insider 	■ Low
<ul style="list-style-type: none"> > Destroying hardware of facilities > Holding data hostage 	■ High
<ul style="list-style-type: none"> > Loss due to earthquake > Loss in information due to flood and fire 	■ High
<ul style="list-style-type: none"> > Computer viruses > Trojan horses and worms 	■ Low

Cyber Attacks Faced by Different Departments



Department



IT
Department



Marketing
Department



Operations
Department



Accounts
Department

Number of Cyber Attacks

22 cyber attacks
in last financial
year

18 cyber attacks
in last financial
year

11 cyber attacks
in last financial
year

13 cyber attacks
in last financial
year

Type of Cyber Attacks

- > Phishing
- > Ransomware
- > URL interpretation

- > Phishing
- > SQL injection
- > DNS spoofing

- > Brute force attack
- > Trojan horse
- > Malware attack

Key Takeaway

IT department faced
maximum number of cyber
attacks in last financial year

Organization lost **\$430,900**
in last financial year due to
phishing attacks

Impact of Information Security Loss on Organization

Financial loss to organization

- › Data breaches now cost companies \$4.24 million per incident on average
- › Rapid shift to working remotely during the pandemic likely led to more expensive data breaches
- › Add text here



Reputational loss

- › Information breach can result in loss of customer trust and end of business relationships in certain cases
- › Reputational loss can lead to loss of customers, sales and investors
- › Add text here



Loss of productivity

- › Cyber attack or any other information breach can result in halting of business operations which may lead to productivity loss
- › Data breach can result in loss of time due to non access of data and systems
- › Add text here



Business continuity

- › If it's not managed well, a data breach can do lasting damage to your organization
- › Add text here
- › Add text here
- › Add text here



Financial Impact of Information Security Attacks



Consequences of different types of cyberattack

(average annual cost; figures in US\$ million; 2018 total = US\$13.0 million)

	Business Disruption	Information Loss	Revenue	Equipment Damage	Total Cost By Attack Type
Malware (+11%)	\$ 0.5	\$ 1.4	\$ 0.6	\$ 0.1	\$ 2.6
Web -based attacks (+17)	\$ 0.3	\$ 1.4	\$ 0.6	\$ -	\$ 2.3
Denial-of- service (+15)	\$ 1.1	\$ 0.2	\$ 0.4	\$ 0.1	\$ 1.7
Malicious insiders (+15)	\$ 0.6	\$ 0.6	\$ 0.3	\$ 0.1	\$ 1.6
Phishing and social engineering (+8%)	\$ 0.4	\$ 0.7	\$ 0.3	\$ -	\$ 1.4
Malicious code (+9 %)	\$ 0.2	\$ 0.9	\$ 0.2	\$ -	\$ 1.4
Stolen devices (+12%)	\$ 0.4	\$ 0.4	\$ 0.1	\$ 0.1	\$ 1.0
Ransomware (21%)	\$ 0.2	\$ 0.3	\$ 0.1	\$ 0.1	\$ 0.7
Botnets (+12%)	\$ 0.1	\$ 0.2	\$ 0.1	\$ -	\$ 0.4
Total cost by Consequence	\$ 4.0	\$ 5.9	\$ 2.6	\$ 0.5	\$ 13.0

Key Takeaways

Malware attacks done maximum amount of financial damage to organizations worldwide






Ransomware attacks are expected to grow at 21% in next financial years

Add text here

Current Information and Data Security Capabilities of Firm



Risk Management Functions






	Description	Required Standard Rating	Actual Standard Rating
 Identify	Identification of assets and information security risk associated with them	4	2
 Protect	Protecting and safeguarding data from internal and external threats	5	4
 Detect	Detect threat and vulnerability in timely manner to avoid data breach	4	4
 Response	Formulating risk mitigation plan to avoid data loss and security breach	5	4
 Recovery	Formulating recovery plan to assess the data in case of loss due to threat	5	5

MITIGATION

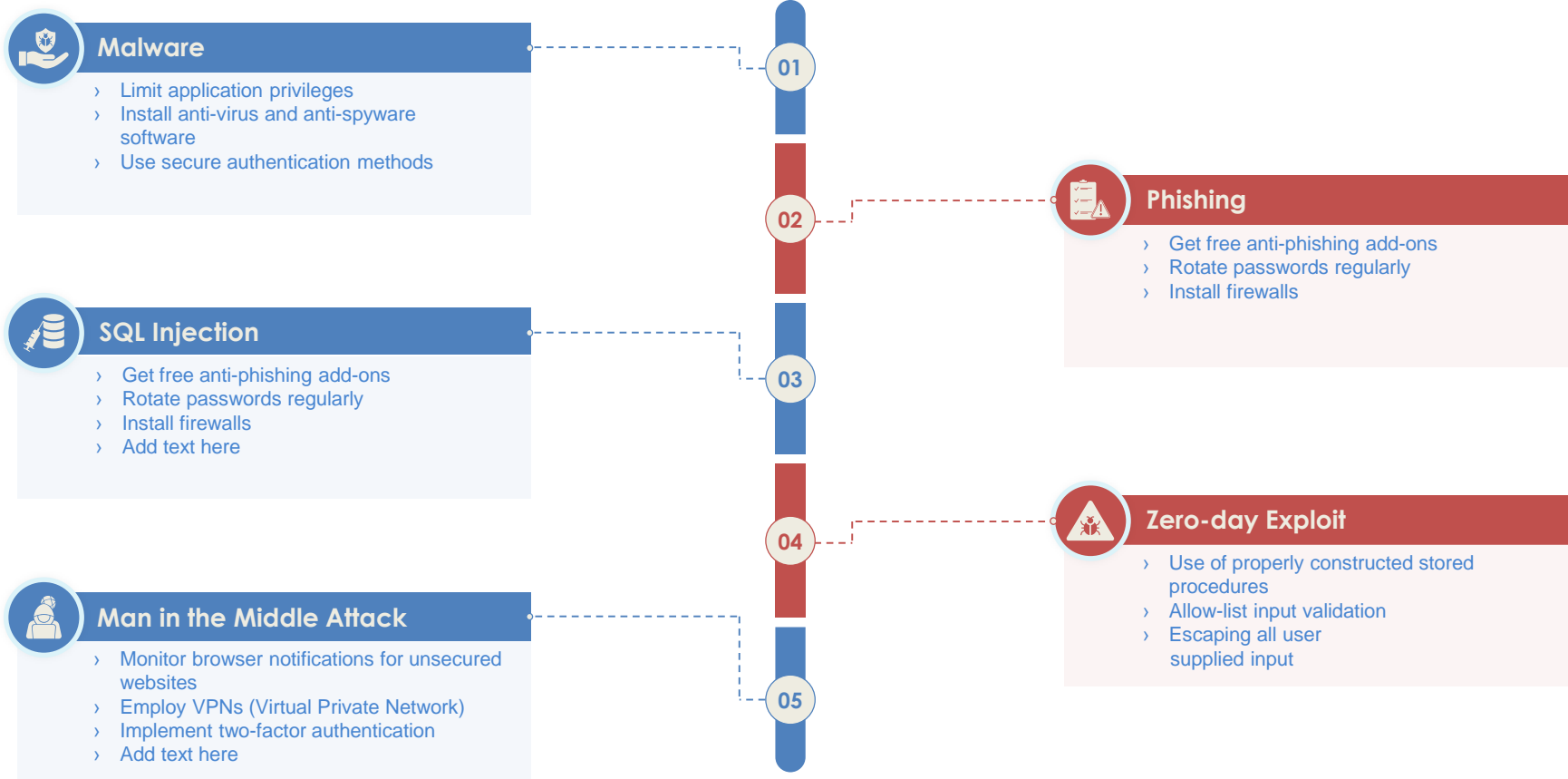
04



Security Breach Risk Management Model

 Asset	 Control Topic	 Evaluation Questions	 Response	 Threat
Server	Use of system credentials	Does customer registration and de registration process is managed efficiently?	No	Misusing system requirements
		Does the management has two unique credentials to perform administer activities ?	No	
		Text here	No	
Database	Database access	Does the multifactor authentication is enabled for administrative access?	No	Data management and leakage
		Text here	No	
Network	Utilization of cryptography in network communication	Does the encryption model is created utilizing good sources for weak keys minimization?	No	Text here
		Text here	No	
Application	Exception handling	Does the error messages by system generation model are sanitized to reveal minimum insights	No	Platform
Cloud	Cloud configuration	Text here	No	
		No		

Mitigation Strategies to Tackle Information Security Threats



Mitigation Plan for Resolving Encountered Threat

	Threat	Risk	Risk Priority	Risk Mitigation Plan	Risk Owner	Expected Resolution Time	Add Text Here
01	Sensitive customer data in cloud services	Loss of customer confidence, reputational damage from data leak	High	Identify customer data in cloud services and encrypt them prior to sending them to the cloud	Departmental IT manager	5 days	Add text here
02	Unpatched web servers	Exploitation weakness in web servers to set a foot in the organization's network to steal data	Medium	Inventory all the web servers and implement relevant patches	Departmental IT coordinator	8 days	Add text here
03	Lack of security awareness with departmental users	Users falling prey to social-engineering attacks including phishing	High	Identify security behaviors to improve and customize awareness trainings	Senior manager of business operations	7 days	Add text here
04							
05							

Security Risk Management Assessment Checklist



Information Security Policy

1. Information Security Policy Document

- o Does an information security policy exist, which is approved by the management, published and communicated as appropriate to all employees?
- o Does it state the management commitment and set out the organizational approach to managing information security?

2. Review and Evaluation

Does the Security policy have an owner, who is responsible for its maintenance and review according to a defined process?



Security of Third Party Access

1. Identification of risks from third party

- o Are risks from third party access identified and appropriate security controls implemented?
- o Are the types of accesses identified, classified and reasons for access justified?
- o Are secure risks with third party contractors working onsite identified and appropriate controls implemented?



Responding to security/threat incidents

1. Reporting security/ threat incidents

- a) Does a formal reporting procedure exist, to report security/threat incidents through appropriate management channels as quickly as possible?

2. Reporting security weaknesses

- a) Does a formal reporting procedure or guideline exist for users, to report security weakness in, or threats to, systems or services?



Media handling and security

1. Management of removable computer media

- a) Does a procedure exist for management of removable computer media such as tapes, disks, cassettes, memory cards and reports?



Business Requirements for Access control

1. Access Control Policy

- a) Have the business requirements for access control been defined and documented.
- b) Does the Access control policy address the rules and rights for each user or group of users?
- c) Are the users and service providers given a clear statement of the business requirement to be met by access controls?



Exchange of information and software

1. Information and software exchange agreement

- a) Is there any formal or informal agreement between the organizations for exchange of information and software?

Security Risk Assessment Types

*thank
you*



ALASKA NATIVE
TRIBAL HEALTH
CONSORTIUM

Milton Kabia
ISSO/IT Security Director
ANTHC
mkabia@anthc.org

