CBS COPENHAGEN BUSINESS SCHOOL

Selma Schouw | David Hark | Antonia Strobl

OPERATION PULSEWAVE

Case Study - Saga Labs

MSc Business Administration and Data Science

EQUIS ACCREDITED AACSB ACCREDITED AMBA ACCREDITED CEMS PIM

Case Introduction

Selma Schouw | David Hark | Antonia Strobl

(1) **Incident Summary**

(2) **Timeline**

(3) **MITRE ATT&CK Map**

(4) **Threat Attribution**

(5) **Expectations**

(6) **Legal Implications**

(7) **Public Relations**
& Business

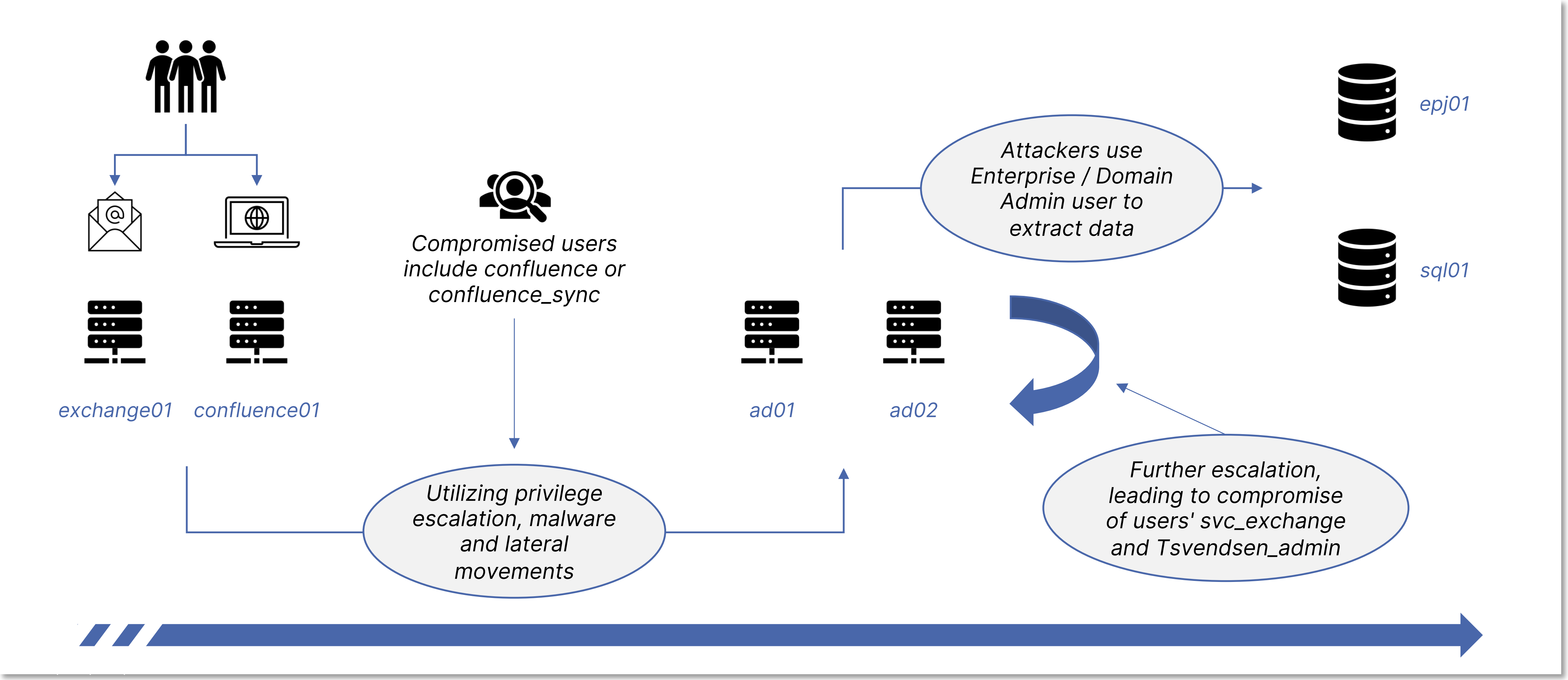
(8) **Systems & Oganization**

1 Incident Report

- Command script used for initial system access.
- Credentials compromised via escalated privileges.
- Evasion tactics detected, indicating deliberate obfuscation.
- Unauthorized network access through malware.
- Persistence established by attackers in systems.
- Data exfiltration setup indicates potential data compromise.
- Organized command and control activity observed.
- Attack pattern aligns with APT group methods.

2 TIMELINE

Summary of Cyber Attack Timeline



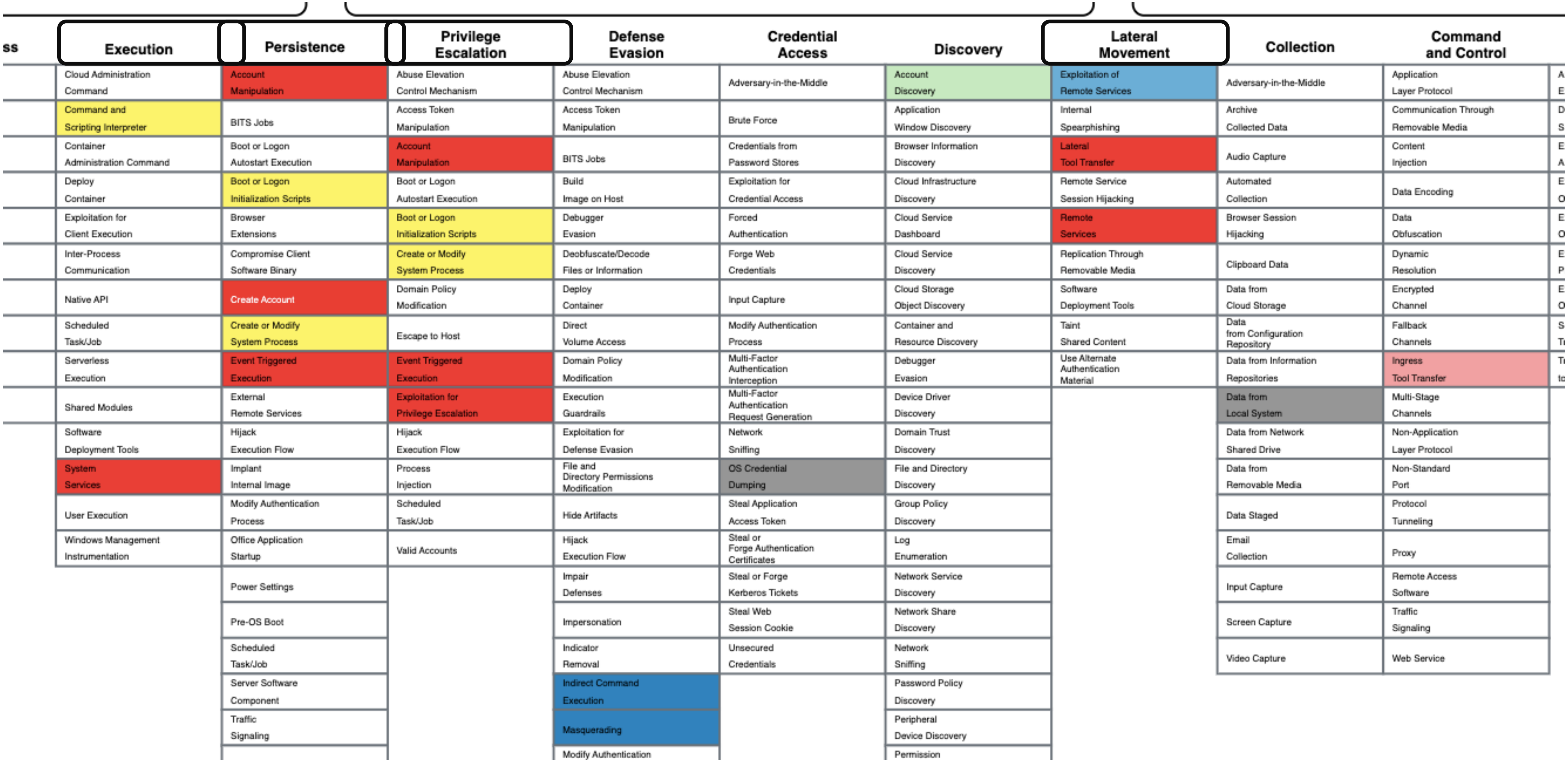
Compromised users include confluence or confluence_sync

Utilizing privilege escalation, malware and lateral movements

Attackers use Enterprise / Domain Admin user to extract data

Further escalation, leading to compromise of users' svc_exchange and Tsvendsen_admin

3 MITRE ATT&CK



ss	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	
	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	A E
	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	D S
	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	E A
	Deploy Container	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	E O
	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation	E O
	Inter-Process Communication	Compromise Client Software Binary	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forge Web Credentials	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	E P
	Native API	Create Account	Domain Policy Modification	Deploy Container	Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel	E O
	Scheduled Task/Job	Create or Modify System Process	Escape to Host	Direct Volume Access	Modify Authentication Process	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository	Fallback Channels	S T
	Serverless Execution	Event Triggered Execution	Event Triggered Execution	Domain Policy Modification	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material	Data from Information Repositories	Ingress Tool Transfer	T t
	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels	
	Software Deployment Tools	Hijack Execution Flow	Hijack Execution Flow	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	
	System Services	Implant Internal Image	Process Injection	File and Directory Permissions Modification	OS Credential Dumping	File and Directory Discovery		Data from Removable Media	Non-Standard Port	
	User Execution	Modify Authentication Process	Scheduled Task/Job	Hide Artifacts	Steal Application Access Token	Group Policy Discovery		Data Staged	Protocol Tunneling	
	Windows Management Instrumentation	Office Application Startup	Valid Accounts	Hijack Execution Flow	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection	Proxy	
		Power Settings		Impair Defenses	Steal or Forge Kerberos Tickets	Network Service Discovery		Input Capture	Remote Access Software	
		Pre-OS Boot		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Traffic Signaling	
		Scheduled Task/Job		Indicator Removal	Unsecured Credentials	Network Sniffing		Video Capture	Web Service	
		Server Software Component		Indirect Command Execution		Password Policy Discovery				
		Traffic Signaling		Masquerading		Peripheral Device Discovery				
				Modify Authentication		Permission				

3 MITRE ATT&CK

TACTICS

(1) Execution

(2) Persistence

(3) Privilege Escalation

(4) Defense Invasion

(5) Credential access

(6) Discovery

(7) Lateral Movement

(8) Collection

(9) Command and Control

TECHNIQUES

(1) Command and Scripting Interpreter

(2) System Services

(3) Account Manipulation

(4) Boot or Logon Initialization Scripts

(5) Create account

(6) Create or Modify system process

(7) Event Triggered Execution

(8) Exploitation for Privilege Escalation

(9) Indirect Command Execution

(10) Masquerading

(11) OS Credential Dumping

(12) Account Discovery

(13) Exploitation of remote services

(14) Lateral Tool Transfer

(15) Remote services

(16) Data from local system

(17) Ingress Tool Transfer

PROCEDURES

(1) PowerShell

(2) Service Execution

(3) Windows Service

(4) SMB/Windows Admin Shares

(5) Upload to remote server

4 THREAT ACTOR ATRRIBUTION

WHY

Data

- Patients.rar - Patient Information
- NATO – use for blackmail, espionage, sabotage

➔ Political motivation

Monitary

- Passwords – sold online

➔ Financial motivation

WHO

Strategy

- leave system running
- hide identity
- quick

Traces

- FDP server in Hong Kong
- Data upload Attempt

Suspects

Cozy Bear – APT29

- Russia's Foreign Intelligence Service (SVR)
- Targeting government networks in Europe and NATO member countries, research institutes, and think tanks

Wicked Panda – APT41

- Chinese state-sponsored
- Espionage and financial objectives
- Targeting healthcare, technology, gaming

4 THREAT ACTOR ATRRIBUTION

Cozy Bear – APT29

TACTICS
Privilege Escalation
Lateral Movement
Command Control
Defence Invasion
Collection

TECHNIQUES
Account Discovery
Scanning
Account Creation
Malware e.g. mimikatz
Masquering

Wicked Panda – APT41

TACTICS
Privilege Escalation
Lateral Movement
Command Control
Defence Invasion
Collection

TECHNIQUES
Data from local system
Masquerading
System Information
Discovery
Windows Management
Instrumentation

CBS

4 THREAT ACTOR ATRRIBUTION

WHY

Data

- Patients.rar - Patient Information
- NATO – use for blackmail, espionage, sabotage

➔ Political motivation

Monitary

- Passwords – sold online

➔ Financial motivation

WHO

Strategy

- leave system running
- hide identity
- quick

Traces

- FDP server in Hong Kong
- Data upload Attempt

Suspects

Cozy Bear – APT29

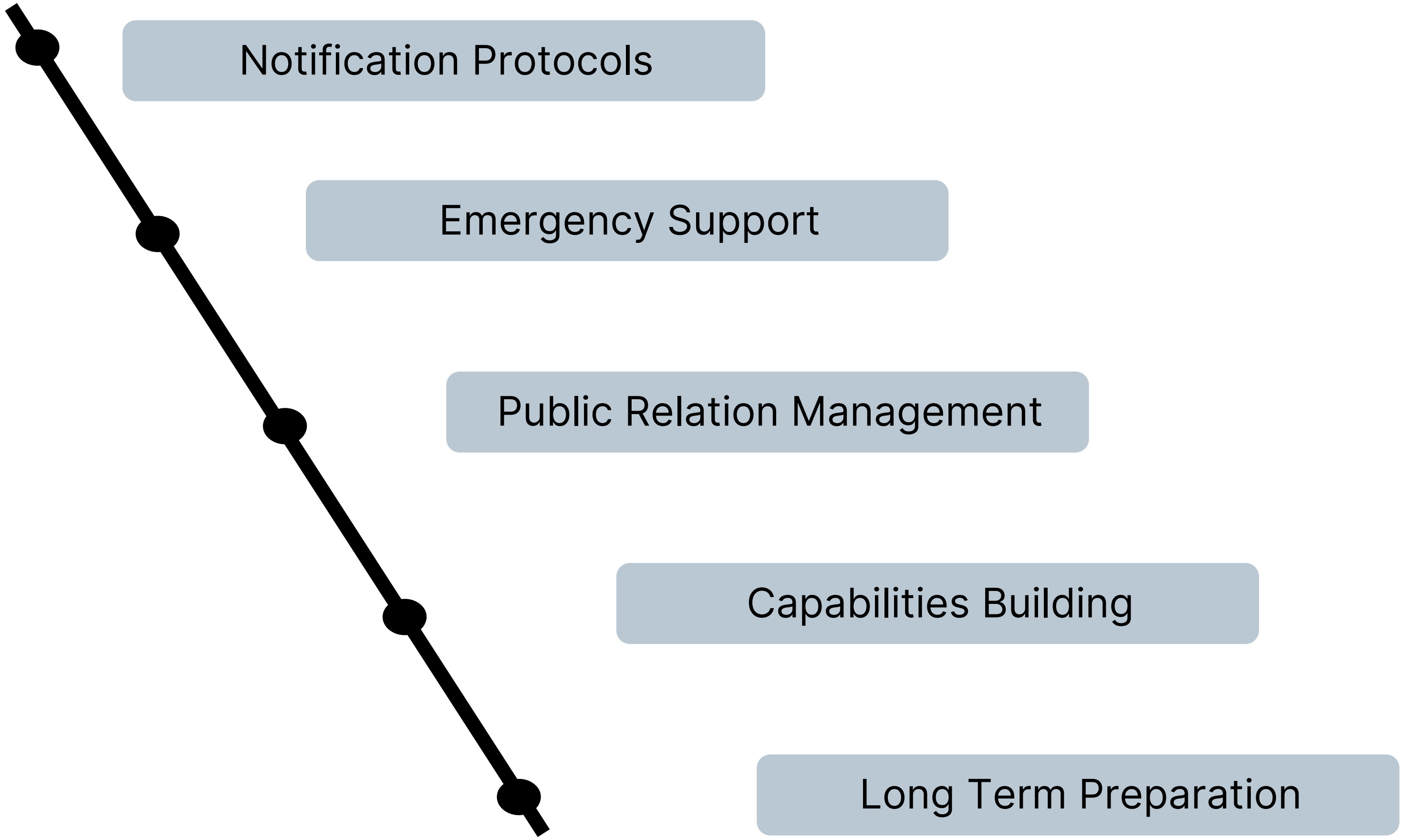
- Russia's Foreign Intelligence Service (SVR)
- Targeting government networks in Europe and NATO member countries, research institutes, and think tanks

☆ Wicked Panda – APT41

- Chinese state-sponsored
- Espionage and financial objectives
- Targeting healthcare, technology, gaming

CBS

5 Expectations



Notification Protocols

Emergency Support

Public Relation Management

Capabilities Building

Long Term Preparation

6 Legal Implications

Legal Assessment under GDPR

Priority level: **High**

- Must immediately notify supervisory authorities and affected data subjects (art. 33 & art. 34)
- Re-evaluation of cyber security to adhere to GPDR

Legal Liability Analysis

Priority level: **Medium**

- Acquire legal assistance to mitigate the damages to the hospital with legal proceedings

7 Public Relations & Business

Emergency Support

⚠ Priority level: **Medium**

- Contact in case of further extortion
- Legal advice
- Bridging contact with mental health organizations

Long-term Strategic Planning

⚠ Priority level: **Low**

- Campaign with Danish public hospitals that seeks to build trust surrounding their cybersecurity measures
- Review by external cybersecurity company

Priority level: **High**

8 Systems & Organization

System

Priority level: **Medium**

- Constant Monitoring of Alerts
- Strengthening of weak points
- Periodic Controls for possible weaknesses

Organization

Priority level: **Low**

- Establish emergency plans and procedures
- Establish responsibilities and communication channels
- Practice extreme cases

CBS COPENHAGEN BUSINESS SCHOOL

THANK YOU

End of presentation

EQUIS ACCREDITED AACSB ACCREDITED AMBA ACCREDITED CEMS PIM