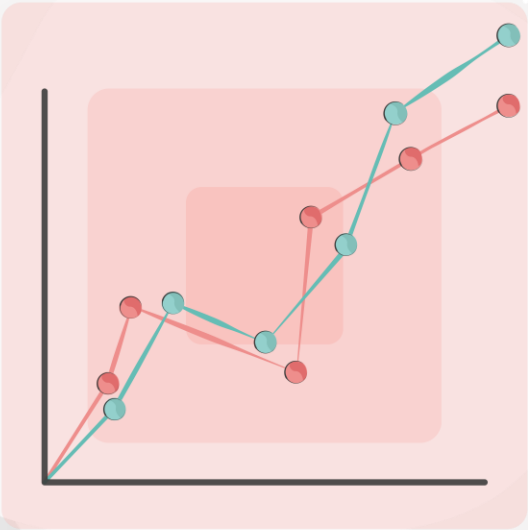
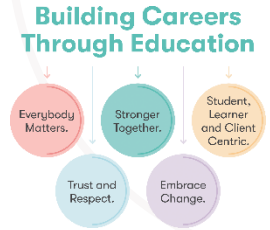
Level 5 Data Engineer
Module 4 Topic 4

Security policy and incident response

Welcome to today's webinar.

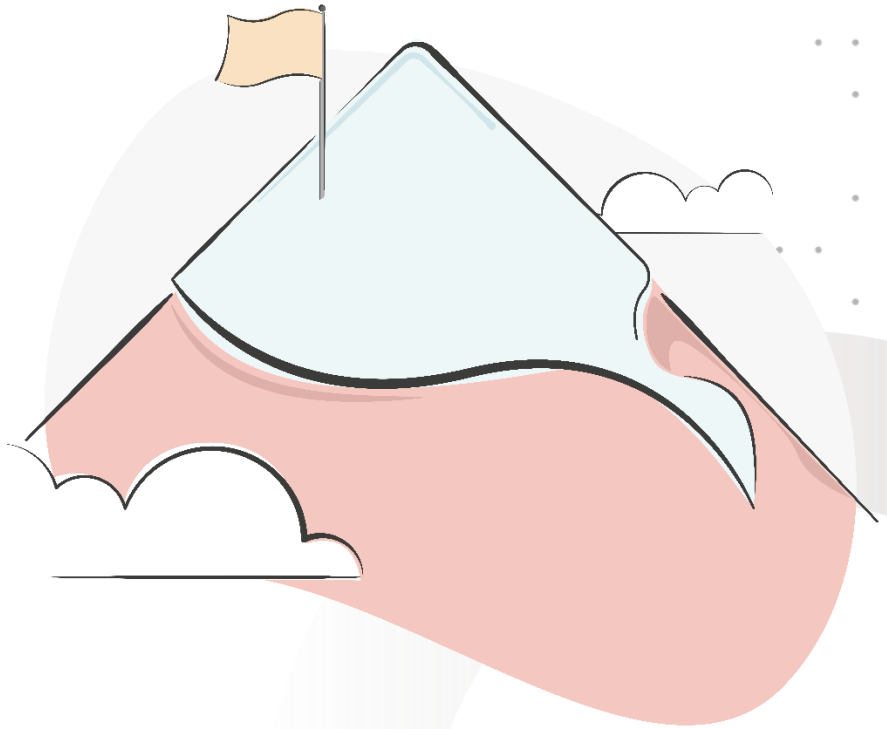


Session aim and objectives



This webinar supports the following learning outcomes:

- Explain the importance of security policies and established policy frameworks in keeping data products and pipelines secure
- Implement risk mitigation strategies and remediation techniques to address potential security breaches.
- Document and learn from security incidents to enhance future response strategies.
- Identify various types of security policies and their applications to enhance organisational security.



BPP

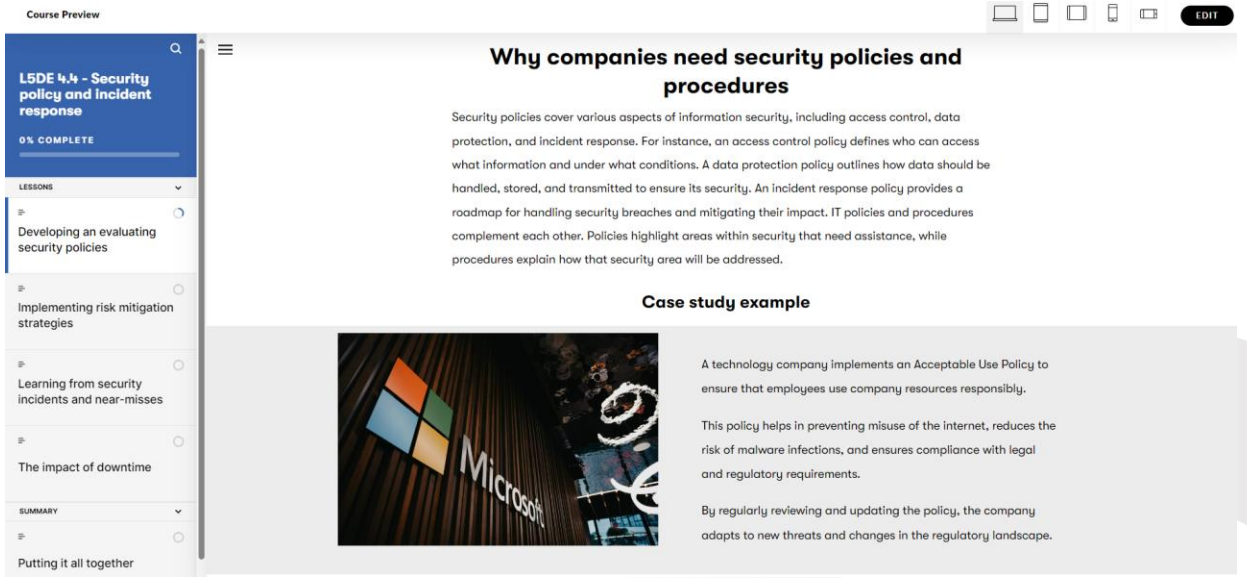
Recap of e-learning

Building Careers Through Education

Everybody Matters. Stronger Together. Student, Learner and Client Centric. Trust and Respect. Embrace Change.

Are you happy with your learning?

- What do we mean by ‘risk mitigation’?
- What risk mitigation strategies do you recall?
- List the different types of security polices that you remember.
- What is the impact of downtime?



A screenshot of topic 4 e-learning

BPP

Webinar Agenda

What we will cover in the webinar:

1. **Deep Dive into the CIA Triad**

- Explore the core principles of Confidentiality, Integrity, and Availability in cybersecurity.

2. **Cryptography basics**

- How cryptography can aid confidentiality

3. **NIST Cybersecurity Framework**

- Introduce the NIST framework and its core functions for comprehensive security management.

What we will cover in the webinar:

- **Monitoring Practices and Open-Source Frameworks**
  Discuss the importance of continuous monitoring and explore open-source security tools to help integrity and availability

- **Binary Risk Assessment**
  Explain the concept of binary risk assessment and demonstrate its application.

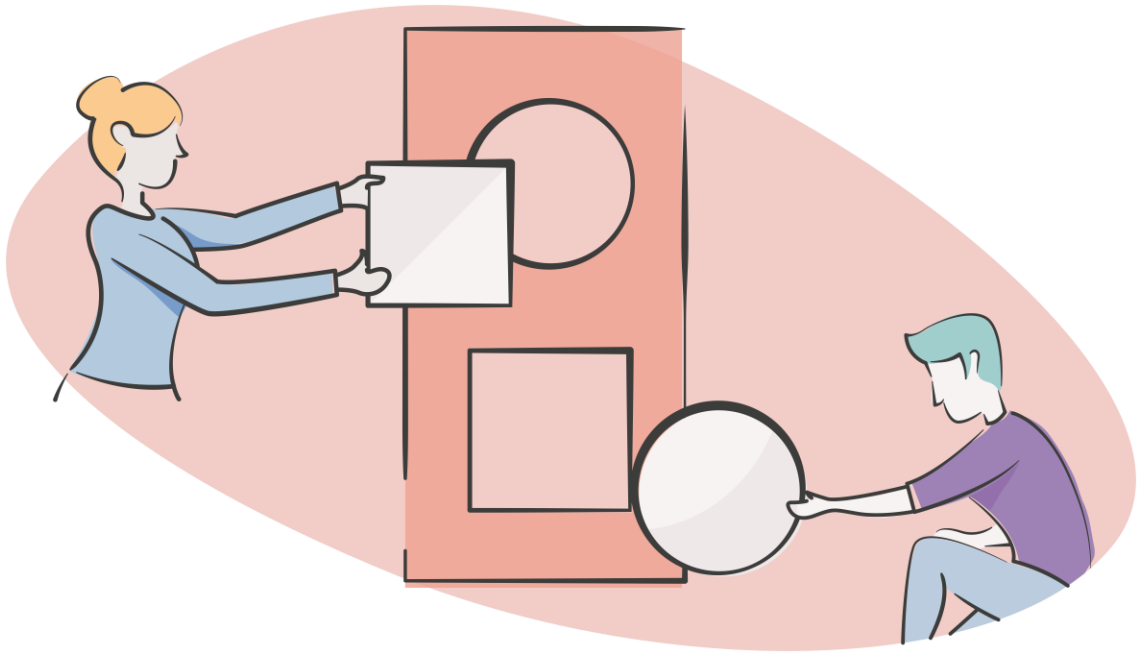
- **Case Study: Financial Impact of a Security Breach**
  Analyze the financial implications of a security breach and the importance of risk mitigation..

BPP

Lab Activity

Worksheet review and discussion

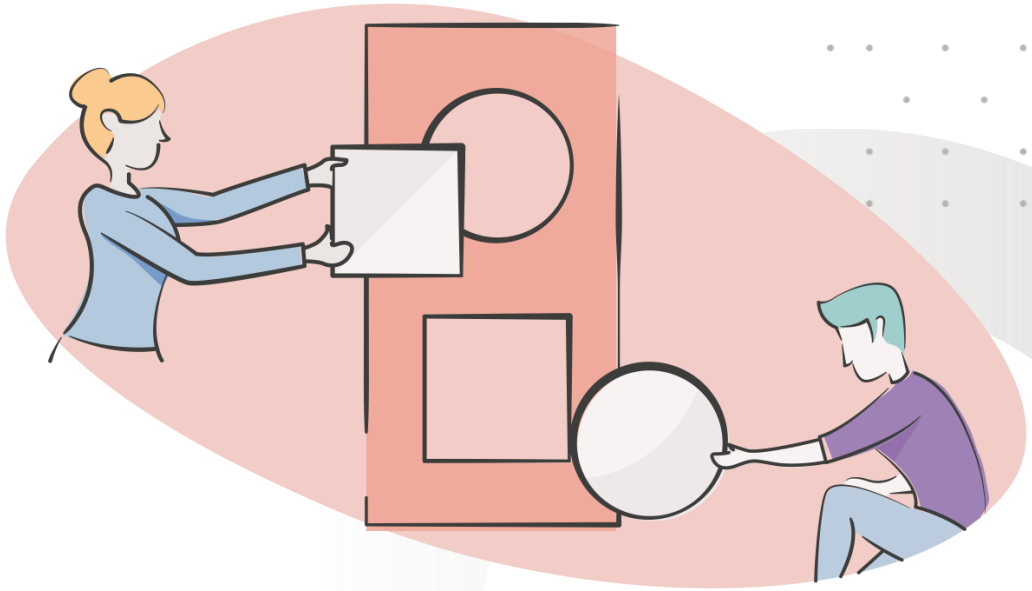
Review the worksheet for Topic 3 (anti patterns and security risks) and complete the group-based discussion activity.



Activity

Group research

- Use Google and LinkedIn to research the role of “Security Architect?
- What do they do?
- Do you know any in your organisation?



Security architectures

The solution…

- Security architects develop the overall **security strategy,** as well as individual **designs for secure systems and networks.**

- They create **policies, standards, procedures, and documentation** designed to work across all departments and for all applications..

- As a result, they **need to have a working knowledge about many different system components**: information security programs, IT operations, and identity and access management.

They also develop incident response plans and manage risks.

BPP

Incident response

What is it…?

Incident:

- An action likely to lead to grave
- consequences especially in diplomatic
- matters <a serious border incident>

Grave consequences:

- Sounds bad. Really bad. Probably does
- not look good on the resume.
- Could mean loss of revenue.
- Company/Corporate level.
- Personal level.

BPP

Incident examples

Malicious code.

- Virus infection.
- Trojan programs.
- Worms.
- Malicious scripting.

Usually hidden and some have the potential to Replicate.

Effects can range from simple monitoring (spying) on system/network traffic to installing automated backdoors with elevated system rights, allowing the attacker to wreak havoc.

BPP

Incident examples

Malicious code.

Unauthorized Access.

- Accessing data without permission.
- Utilising an account not assigned.
- Utilising another users account.
- Utilising assigned account in a manner not specifically assigned.
- Elevating privileges above assigned.

BPP

Incident examples

Malicious code.

Unauthorized Access.

Unauthorized Utilization of Services.

Game play.

Mail relay.

x Use of corporate equipment for personal gain. (Home business, stocks, etc…)

Personal servers on network.

Much of this can be enforced by well-drafted Policy (what type of policy?

BPP

Incident examples

Malicious code.

Unauthorized Access.

Unauthorized Utilization of Services.

Espionage.

- Information stealing/manipulation.
- Email monitoring.
- Notebook theft.
- Data copying.
- Simple trojan/tunneling methods.

Incident examples

Malicious code.

Unauthorized Access.

Unauthorized Utilization of Services.

Espionage.

Hoaxes.

Warnings.

Virus threats, bomb threats, etc…

Scams.

Pyramid mail, sob stories, contests.

Corporate mail is for Business use *only.*

Authorised personnel will distribute warnings.

BPP

Incident examples

Malicious code.

Unauthorized Access.

Unauthorized Utilization of Services.

Espionage.

Hoaxes.

Aggressive Probes.

- *Does not include port scans.*
- *Baseline network to observe unusual trends.*
- *Unusual activity should be investigated.*
- *Monitor both internal and external network traffic…*

BPP

Incident response

What is it…?

Incident Response:

- An act of responding to an action likely to lead to grave consequences especially in diplomatic matters.

But we do not want a "Knee Jerk" reaction.

- Ideally Incident Response would be a set of policies that allow an individual or individuals to react to an incident in an efficient and professional manner thereby decreasing the likelihood of grave consequences.

BPP

Incident response

The purpose…

Minimise overall impact.

Stopping further progression of the incident is key.

Discuss the pros and cons of:

- Hiding the incident from public scrutiny?
- Involving senior staff?

BPP

Incident response

Zoom in on the ‘lingo’…

- What is the difference between threat **mitigation** and **threat remediation**?
- Mitigation includes reducing the impact of a threat when it cannot be eliminated.
- Remediation completely removes the threat when it's possible

BPP

Incident response

Additional purpose…

Recover Quickly & Efficiently.

- Respond as if going to prosecute.
- If possible "replace" the affected system with new one (fail over).
- Priority one, business back to normal.
- Ensure all participants are notified.
- Record everything.

BPP

Incident response

Additional purpose…

Minimise overall impact.

Recover Quickly & Efficiently.

Secure the System.

- Lock down all known avenues of attack.
- Assess system for unseen vulnerabilities.
- Implement proper auditing.
- Implement new security measures.

BPP

Incident response

Additional purpose…

Minimize overall impact.

Recover Quickly & Efficiently.

Secure System.

Follow-up (It is never REALLY over).

- Ensure that all systems are secure.
- Continue prosecution.
- Securely store all evidence and notes.
- Distribute lessons learned.

BPP

Recognising an incident

Automated Response.

- Intrusion Detection System(s)
- Anti-malicious code software.
- Firewall.
- Other security systems.

Log files.

Recognising an incident

Obvious.
Automated Response.
Outside Source.
Physical Report.

System Administrator Report.

- Unusual log activity.
- Failed logins, unusual connect times.
- New accounts.
- New files.
- Missing files.

BPP

Policy

Much of the incident response will depend on your security policy…

Don’t have one? Review previous week.

Hard for employee to deny wrongdoing when you have signed papers showing review of existing policies to include Acceptable Use.

BPP

What is ‘non-repudation’?

Zoom in on the ‘lingo’…

- Nonrepudiation means that if the system says that something happened, then it did happen.

- Nonrepudiation is a concept of trusting the origin, authenticity and integrity of data.

BPP

Policy?

Much of the incident response will depend on your security policy…

Acceptable Use Policy.

- Games?
- Email.
- Personal software?

BPP

Policy?

Much of Incident Response will depend on your Security Policy…

Acceptable Use.

Monitoring.

- Specify daily monitoring for troubleshooting.
- Specify ALL traffic WILL be monitored.

- Do not allow legal opening for invasion of privacy.
- Workplace is for business and all business efforts are subject to security measures and perusal to ensure best business practices.

BPP

Policy?

Much of Incident Response will depend on your Security Policy…

Current Point Of Contact List.

- Primary number for 24 hour emergency.
- Email and desk numbers for Security staff.
- Designed to give all personnel the minimal needed information to respond to an incident or to ask a question.

BPP

Policy?

Much of Incident Response will depend on your Security Policy…

Current Point Of Contact List.

User Responsibilities.

- Acceptable use.
- Software installation.
- Security reporting.
- Be aware (weakest link theory is in full effect for security).

BPP

Policy?

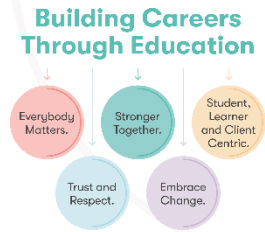
Obvious.

Current Point Of Contact List.

User Responsibilities.

Technician/System Administrator Responsibilities

- Security Officer(s)/Manager(s) Responsibilities.
  - Lead by example.
  - Monitor logs/reports.
  - Provide for on call duties.
  - Open door/email policy.
  - Communicate.
  - Educate the masses.
  - Educate self daily.
  - Be aware (or be compromised).



BPP

Educate

Policy is worthless unless implemented.

- What good is a library that is locked?
- What good are laws that are not enforced?
- What good is a policy that is not updated?

BPP

Educate

Policy is worthless unless implemented.

- The users must have easy access to policy.
- All new users should be required to read
- Policy at hire and sign acceptance.
- Policy should be kept easily available.
    - Online (Read only).
    - Hard copy (HR, Security Office,Library, etc…)
- A system for suggestions should be available.
- All memorandums that affect security should be included in Policy.

BPP

Educate

Policy is worthless unless implemented.

The users must have easy access to the Policy.

- The Policy needs to be explained to users.
- A glossary should be provided.
- The Policy should be easily understandable.
- The Policy should not be vague enough to allow misinterpretation.
- Security should be willing to assist users.
- Every 6 months refresher should be required.
- Coincide with password change.
- Sign for new password and Policy acceptance.

BPP

Educate

Policy is worthless unless implemented.

The users must have easy access to policy.

The policy needs to be explained to users.

- The policy needs to be supported by Management.
- The highest level needs to sign off on policy.
- All members are subject to policy.
- It is at the higher levels that the larger
- “Incidents” can be found.
- “Iron Clad” policies backed by weak enforcement won't work.

Discussion

A security scenario

Time: 8:13 pm

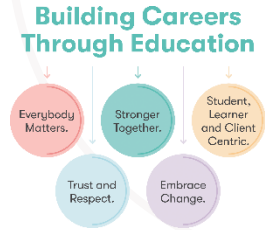
- A V.P. is giving a party at home.
- Decides to show off new web page.

While viewing corporate leadership page V.P.

Notices:

- Certain pictures of persons (including V.P.)
- Bio information have been modified to be less than favourable.

Discussion



A security scenario

Time: 8 15 pm

- Having just read and signed off on the current Security Policy earlier that week.
- V.P. remembers that personnel can contact the helpdesk 24 hours a day for reporting problems.
- Phoning the Helpdesk he reports the problem and

expresses an intense desire to have the situation resolved as soon as possible.

After logging all information the Helpdesk assures the V.P. resolution shall be swift.

BPP

Discussion

A security scenario

- Basic Information to gather:
- Time and date reported (specify time zone)
- Name of contact.
- Phone number and/or email of contact.
- System suspected to be affected.
- Technical details of system if known.
  - IP address(es), OS, patches loaded, physical location, services running, suspected access point (vulnerability).
- Time and date ‘incident’ noticed by contact.
- Description of incident.

Discussion

A security scenario

- Time: 8:20 pm
- Helpdesk finishes entering information into log.
- Helpdesk verifies that page has been modified.
- Per security policy all incidents affecting the company in a ‘Public’ manner are considered Priority 1.

Discussion

A security scenario

- Time: 8:21 pm
- Helpdesk reviews POC list and calls the Security Manager’s pager.
- This specific Sec Manager insists on notification of all Priority 1’s.
- Another approach would be an on-call security member that updates the Manager after reviewing situation.

Discussion

A security scenario

Time: 8:27 pm

Helpdesk reviews POC list and calls the Security Manager's pager.

After being updated of current situation SM requests helpdesk to contact NT server on call person and have him meet him at office in 30 minutes.

SM gets ready for a late night at the office.

Discussion

Scenario 1

Time: 8:30 pm

- Helpdesk checks POC list and calls on call SA.
- Helpdesk explains basic situation to SA.
- SA assures he is getting ready to go.

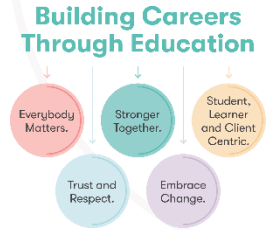
Discussion

Scenario 1

Time: 11 pm

- SA finishes restoring webserver data and verifies that data restored has not been manipulated.
- Since current backup policy states full backups at 0100 every day this gives a roughly 18-hour window for the data manipulation to have occurred.
- SA brings new server online and updates logs for Incident.

Discussion



Scenario 1

Time: 8 am next day

Good news! Through the diligent work of the SA and SM information was found that showed that the data was manipulated at 1957 by a VPN account.

This shows that the incident may have remained unseen by public.

Discussion

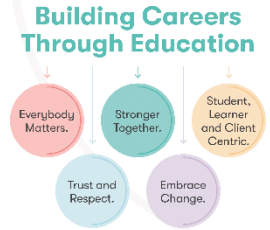
Scenario 1

Time: 8 am next day

- Coordination with HR reveals that the owner of the account had recently been passed over for a promotion.
- Normally that user account would not have rights to the webserver directories but an earlier update to the server created a hole for internal users.
- The SA quickly reconfigured file access for the server and closed that hole.

BPP

Discussion



Scenario 1

Time: 10 am next day

Coordination with HR, Legal, and the employee's direct supervisor showed that due to previous poor work record and misconduct it would be in the best interest of the company to terminate the employment of the individual in question.

- Was this incident response properly executed?
- Would you have changed anything?

BPP

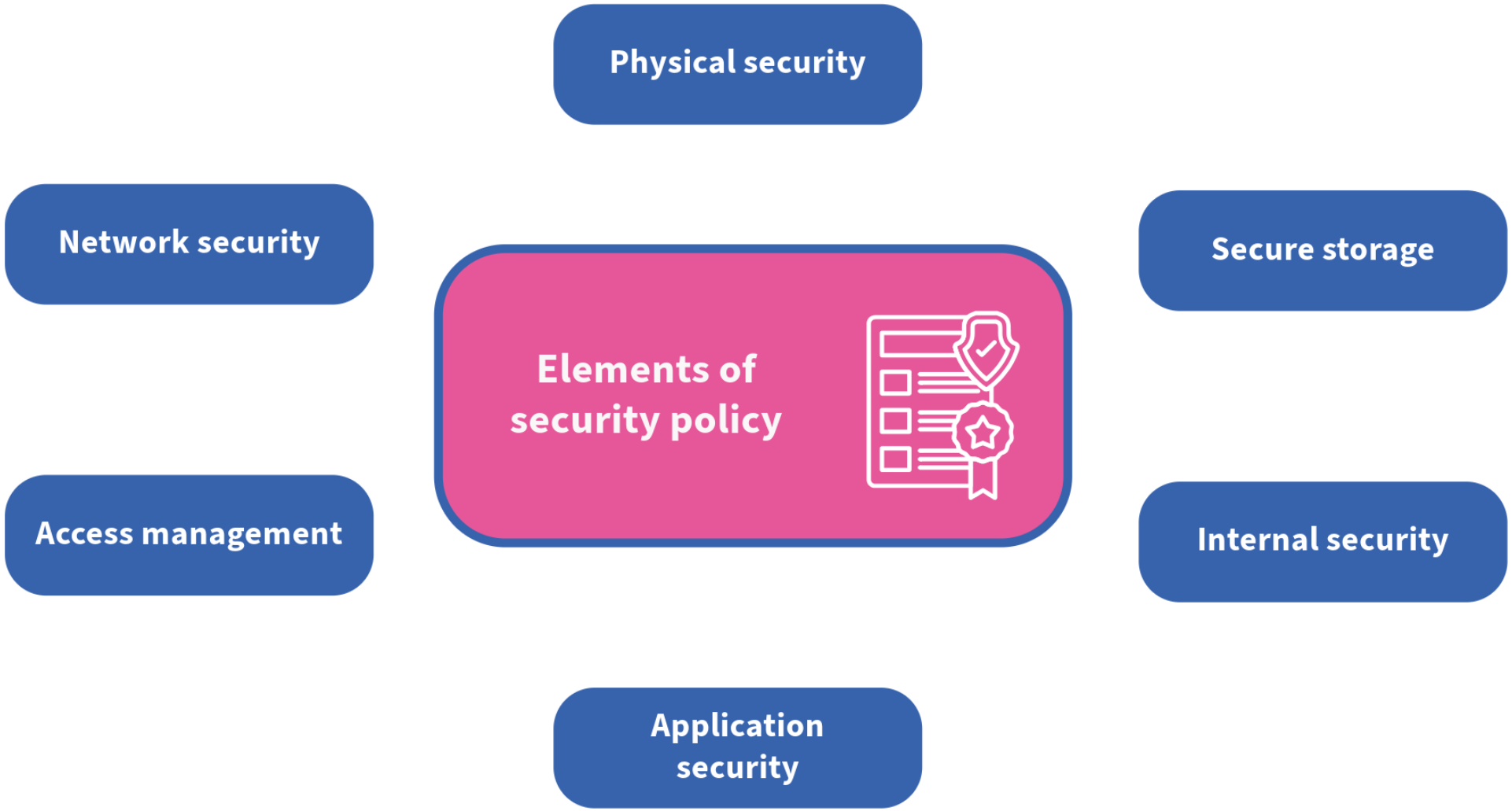
Conclusion

- Due to proper procedures and quick response of all personnel involved the incident was quickly contained, resolved, and business returned to normal.
- Communication and coordination is especially important in Incident Response.
- Any break down in the chain can cause the entire process to fail.

BPP

Security policy

The key elements

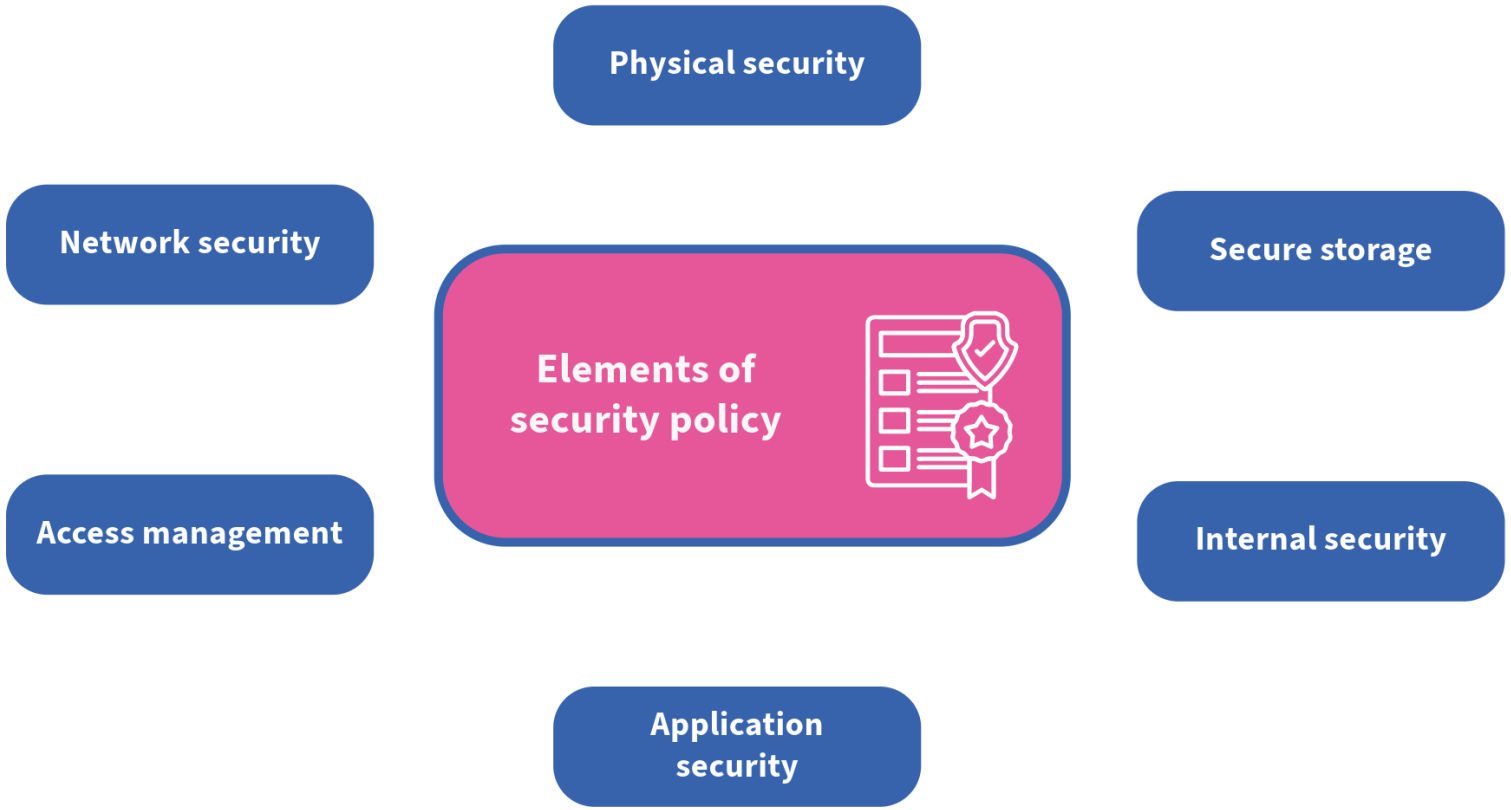


Discussion

Building Careers Through Education

Everybody Matters. Stronger Together. Student, Learner and Client Centric. Trust and Respect. Embrace Change.

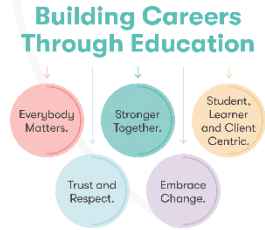
Which of these aspects of security policy do you think employees most commonly overlook?



Submit your responses to the chat!

BPP

Discussion



How would you enforce a policy?

What are the strengths and weaknesses of Jeff Bezos's mandate?

How about the strengths and weaknesses of how he communicated his mandate?

Jeff Bezos' Big Mandate

(circa 2002 — paraphrased)

1. All teams will henceforth expose their data and functionality through service interfaces.
2. Teams must communicate with each other through these service interfaces.
3. No other communication is allowed other than service interfaces over the network.
4. It doesn't matter what technology they use.
5. All service interfaces must be designed to be **externalizable**.
6. Anyone who doesn't do this will be fired.

https://plus.google.com/+RipRoward/posts/eVeouesvaVX

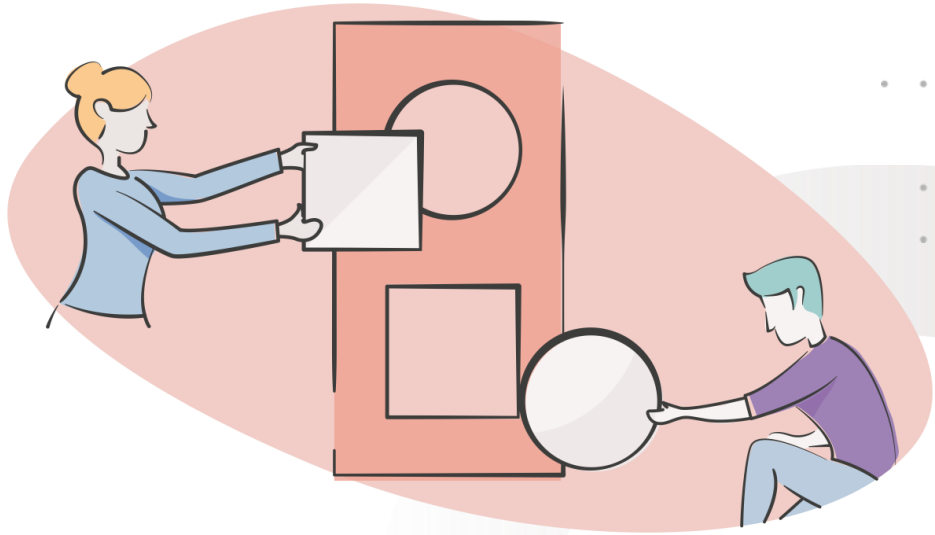
Submit your responses to the chat!

BPP

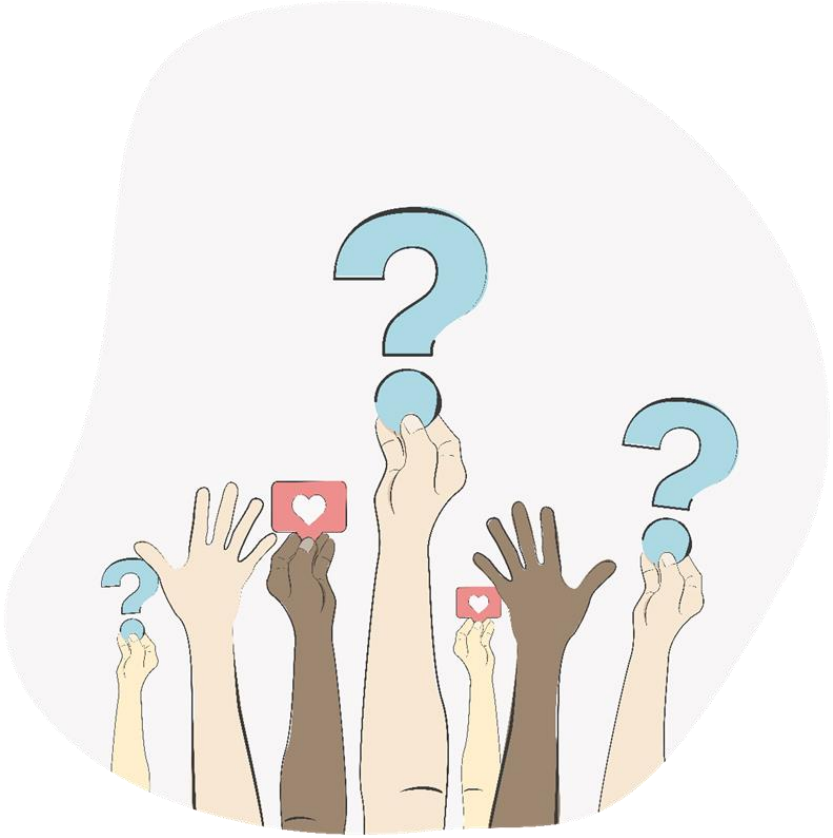
Lab

See the worksheet (Word document) file

Your tutor will guide you through the consolidation of the material from this Module.



Session wrap-up



Any questions or feedback?