Team Infosec

& why we need you

Erica Anderson
@sputina

I’ve worn multiple hats (or jerseys)

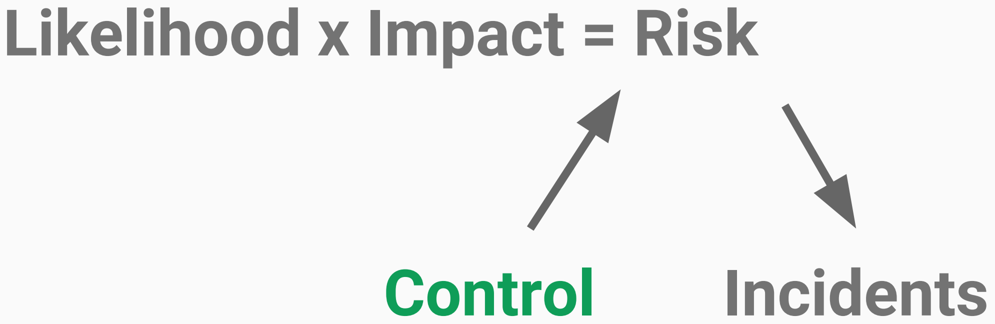
- IT auditor / consultant
- IT security consultant
- Cloud security engineer
- IT security analyst
- Incident response manager
- Workshop instructor
- Programming teacher (for primary school kids)
- Family IT support

… but I am not formally trained

- Bachelor / Master’s degree in Accounting
- Certified Public Accountant (+ a CISA certificate)
- Learned what I know through being a huge nerd

Learning the formula

1. Testing controls
2. Understanding processes
3. Understanding risk



Likelihood x Impact = Risk

Control

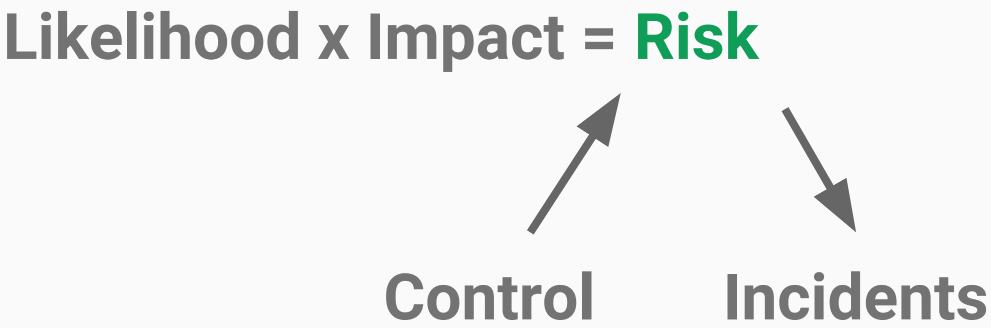
Incidents

Common IT Risk:

Information system that is used in a key financial process is:

- inappropriately changed
- inappropriately accessed
- not available

which results in inaccurate and untrustworthy financial statements.



Likelihood x Impact = Risk

Control

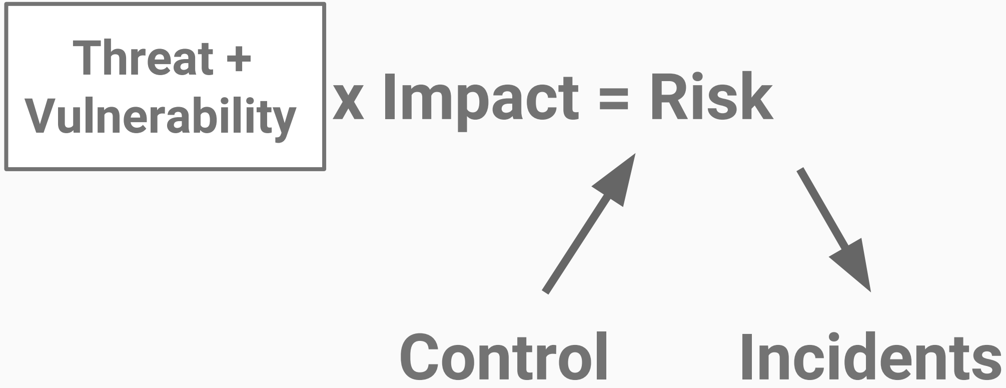
Incidents

Common IT Security Risk:

Information system that is used in a **business** process is:

- inappropriately accessed **by an internal staff member with unnecessary administrative privileges**

which results in a **compromise to the integrity of the data and impacts the organisation's operations.**



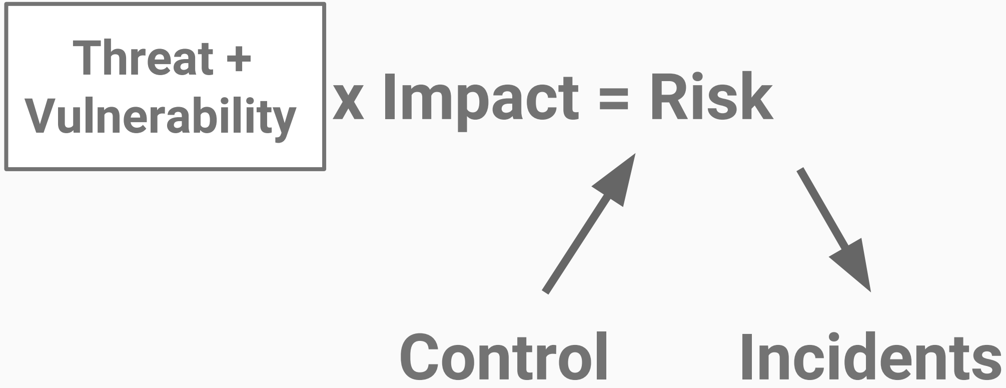
Threat + Vulnerability x Impact = Risk

Control

Incidents

Common IT Security Risk:

- Internet-accessible systems or services & opportunists
- Mistakes by administrators or other internal staff
- Poor security hygiene by end users



Threat + Vulnerability x Impact = Risk

Control

Incidents

Sharing is caring!

Knowledge is power!

1. Controls are not checklists.

Without business context, you don't know the risk.

Without the risk, there is nothing for controls to... well control.

For example: Password age could be a required control - but what risk is it addressing?

2. Compliance are bowling bumpers, not bowling pins.

They are usually are created through bad incidents.

They often act as a baseline of minimum effort.

3. Control or vulnerability findings need context too.

If a control fails in an audit or if a vulnerability is found in a technical test, use context to explain it.

Explain in clear english the factors of the vulnerability (ease of discovery, ease of exploit, awareness).

Explain the risk in detail so the owner knows why it is important.

4. Focus more on quantifying risks than coloring them.

Risk matrices and ratings are only helpful for summarising importance of a risk.

You need to quantify a risk before you can determine how important it is to address.

Spend less time on rating risks and more time understanding what drives the threat, vulnerability, and (technical + business) impact.

5. Empathy & negotiation are important skills to learn.

100% secure is not achievable.

Aim to get as close as possible, while understanding the users who need to navigate the controlled environment.

6. Draw it out!

Use simple diagrams to draw out your understanding of a technical stack.

Use these diagrams to identify how different users access each component, how components talk to each other.

7. Focus less on security products and more on processes.

Security products (like SIEM, WAF, CASB) are not useful if there are no effective processes or basic hygiene.

Spend more time understanding processes behind patching, device hardening, access management, authentication, backups, and logging.

8. Ask questions.

Technology is moving fast, and it is inherently broken.

Take the time to read about what is going on, meet people from other areas of IT and security, ask questions.

Team Infosec needs dedicated:

Developers
Engineers
Analysts
Testers
Auditors

So come join us!

Thanks!

Erica Anderson
@sputina