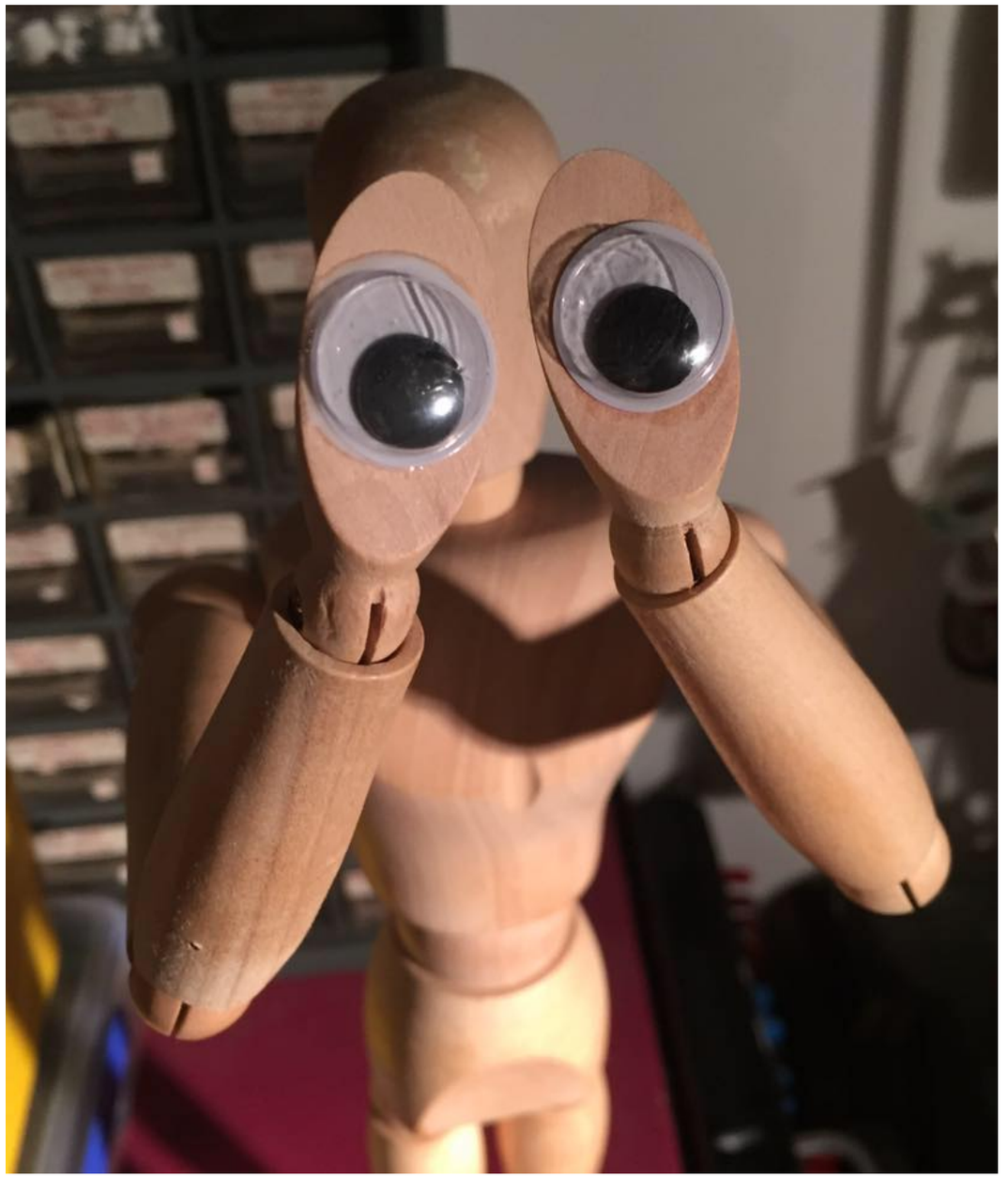
That Vulnerability Looks Quite Risky

Peter Jakowetz - Quantum Security
February 2019

Who am I?

- Security Consultant - Quantum Security WGN
- CISSP, CISA, OSCP, PCI QSA
- Electrical engineer by training
- Work primarily in GRC
- Break electronics, work on cars and play with my cat



Agenda

- Why am I here?
- What’s a risk?
- Why would I use risks?
- How to write a risk
- Benefits
- Useful resources

Why am I here?

- Technical findings are great!
- We have all the findings
- No one will fix the findings… not even one of them
- Risks can be a useful way to describe these findings, quantify them, and fix them
- As engineers we like to fix everything, immediately, using the technical solution, sometimes there’s another way

What is risk management?

“Information **security risk management** is the process of **managing risks** associated with the use of information technology. It involves identifying, assessing, and treating **risks** to the confidentiality, integrity, and availability of an organisation's assets”

What is a risk

- A risk is the intersection of assets, threats and vulnerabilities - “The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability”

- An asset is what we’re trying to protect

- A threat is what we’re trying to protect against - Anything that can exploit a vulnerability intentionally or accidentally

- A vulnerability is a weakness or gap in our protection efforts - Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorised access to an asset

Why do I care?

- We can use risks to quantify issues
- Business owners understand risk, as business owners understand money
- Not all technical issues are equal
- It can help you contextualise & communicate what is or isn’t important

Threat Modelling vs. Risk Assessment

- **Threat modelling** - What are all the things that can go wrong?
- Very useful in the build stage

- **Risk Assessment** - What do those threats mean to your organisation?

- Very useful in build and during the lifecycle

Example Scenario

- You work on a medium size e-commerce website
- You've had a penetration test done and they identified a XSS vulnerability
- You've added it to a register somewhere, but you're not getting any traction getting it fixed - no time, money etc

What’s the risk

- A malicious person runs arbitrary code in a users browser due to a cross site scripting vulnerability in the comments submission field on the ecommerce webpage. This leads to information disclosure, modification and may lead to the loss of private information.

What other information?

- We have the risk statement
- What are the drivers?
- What might it lead to?
- What controls can we put in place?
- How do we quantify (score) this?

What drives this risk?

- XSS vulnerability in the comments section
- No regular testing occurs on the website
- No WAF on the website
- Poor input validation
- Popular website
- Drives a lare amount of company revenue through the website (i.e. reputation)
- Legacy website that we don’t want to push changes to

What might this lead to?

- Loss of personal information by users of the website
- Loss of confidence by users
- Loss of revenue due to reduced confidence in the website
- Reputational damages
- Will this affect Confidentiality, Integrity or Availability of data?

Control Types

- **Deterrent Controls** - i.e. warning screens, security cameras

- **Preventative Controls** - i.e. user account management, firewall rules

- **Detective Controls** - i.e. IDS, monitoring, logging

- **Corrective Controls** - i.e. Data backups, DR plans

What can I do to fix this?

- Web application firewall
- Update CSP
- Conduct input validation
- Static testing of web application for security vulnerabilities
- Regular penetration testing
- Annual penetration testing
- Code review
- Developer training
- Logging
- Change control

Controls

- **CertNZ Critical Controls** - MFA, Patching, Disabling unused services and protocols, Change credentials, Implement app whitelisting, Enforce least privilege, Centralised logging, Network segmentation, Cloud authentication

- **ASD Top 35 Cyber Mitigation Strategies**

Controls

- What of these would make the biggest change?
- What exactly do I want the controls to do?
- Add detail to controls
- Can I roll these together into a single action
- Does one control negate the others?

Scoring

- Likelihood/ Probability - The chance of an event occurring
- Impact/ Consequence - The outcome of an event
- We do this for current state, and future state
- https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/security/

Likelihood

Rating	Description	Meaning
5	Almost Certain	It is easy for the threat to exploit the vulnerability without any specialist skills or resources or it is expected to occur within 1 – 6 months.
4	Highly Likely	It is feasible for the threat to exploit the vulnerability with minimal skills or resources or it is expected to occur within 6 – 12 months.
3	Possible	It is feasible for the threat to exploit the vulnerability with moderate skills or resources or it is expected to occur within 12 – 36 months.
2	Possible but Unlikely	It is feasible but would require significant skills or resources for the threat to exploit the vulnerability or it is expected to occur within 3 – 5 years.
1	Almost Never	It is difficult for the threat to exploit the vulnerability or it is not expected to occur within 5 years.

Impact

Rating	Description	Reputation	Health and Safety	Service Delivery	Financial
5	**Severe**	• The agency suffers severe political and/or reputational damage that is cannot easily recover from. • The Government suffers severe negative reputational impact, and the Prime Minister loses confidence in the Minister and/or the agency's senior management. • Minister and Chief Executive need to be briefed and regularly updated. • Media interest is sustained for a prolonged period (i.e., over a week) with major criticism levelled at the Minister and/or the agency. • The agency breaches multiple laws, which leads to legal action by affected stakeholders. • External/independent investigation is commissioned by the SSC, GCIO or OPC. • The SSC and GCIO manage the communications and recovery.	• Loss of life. • Major health and safety incident involving members of staff and/or members of the public. • The injured party or parties suffer major injuries with long-term effects that leave them permanently affected. • An external authority investigates the agency's safety practices and the agency is found to be negligent.	• Severe compromise of the strategic objectives and goals of the agency. • Severe compromise of the strategic objectives of the NZ Government or other agencies. • Severe on-going impact on service delivery across NZ Government or multiple agencies. • Skills shortages severely affect the ability of the agency to meet its objectives and goals. • Staff work hours are increased by more than 50% (20 hours per week) for more than 30 days. • Between a 10% or more increase in staff turnover in a six-month period that can be directly attributed to the risk eventuating	• Impact cannot be managed without additional funding from government. • Impact cannot be managed without significant extra human resources. • Yearly operating costs increase by more than 12%. • One-time financial cost greater than $100,000.
4	**Significant**	• The agency suffers significant political and/or reputational damage. • Minister suffers reputational damage and loses confidence in the agency's senior management. • Minister and Chief Executive need to be briefed and regularly updated. • Media interest is sustained for up to a week with minor criticism levelled at the agency. • Key stakeholders need to be informed and kept up to date with any developments that affect them. • The agency breaches the law, which leads to legal action by affected stakeholders. • External/independent investigation is commissioned by the SSC, GCIO or OPC. • Communications and recovery can be managed internally with strong guidance from the SSC and GCIO.	• A significant health and safety incident involving multiple members of staff and/or members of the public. • The injured party or parties suffer significant injuries with long-term effects that leave them permanently affected. • An external authority investigates the agency's safety practices and the agency is found to be inadequate.	• Significant compromise of the strategic objectives and goals of the agency. • Compromise of the strategic objectives of the NZ Government or other agencies • Significant on-going impact on service delivery across one or more business unit or multiple agencies. • Skills shortages affect the ability of the agency to meet its objectives and goals. • Staff work hours are increased by more than 38% (10 – 15 hours per week) for 30 days. • Between a 3% and 10% increase in staff turnover in a six-month period that can be directly attributed to the risk eventuating.	• Impact cannot be managed without re-prioritisation of work programmes. • Impact cannot be managed without extra financial and human resources. • Yearly operating costs increase by 10% to 12%. • One-time financial cost between $50,000 and $100,000.
3	**Moderate**	• Agency suffers limited political and/or reputation damage. • Minister is informed and may request to be briefed. • The Chief Executive and senior management need to be briefed and regularly updated. • The agency breaches its compliance obligations. • Media interest is sustained for less than a week with minor criticism levelled at the agency. • Key stakeholders need to be informed and kept up to date with any developments that affect them. • External/independent investigation is commissioned by the agency. • Most communications and recovery can be managed internally with some guidance from the GCIO.	• Health and safety incident involving multiple members of staff or one or more members of the public. • The injured party or parties suffer injuries with long-term effects and are not permanently affected. • The agency's safety practices are questioned and found to be inadequate.	• Compromise of the strategic objectives and goals of the agency. • Moderate impact on service delivery across one or more business unit due to prolonged service failure. • Staff work hours are increased by less than 25% (8 – 10 hours per week) for a two to four week period. • Between a 1% and 3% increase in staff turnover in a six-month period that can be directly attributed to the risk eventuating.	• Impact can be managed with some re-planning and modest extra financial or human resources. • Yearly operating costs increase by 7% to 10%. • One-time financial cost of $20,000 to $50,000.
2	**Minor**	• Senior management and/or key stakeholders believe that the agency's reputation has been damaged. • The Chief Executive needs to be advised. • Senior management needs to be briefed. • Media interest is short-lived (i.e., a couple of days) and no blame is directed at the agency. • Key stakeholders need to be informed. • Communications and recovery can be managed internally.	• Minor health and safety incident involving multiple members of staff or a member of the public. • The injured party or parties suffers minor injuries with only short-term effects and are not permanently affected.	• Minor impact on service delivery across one or more branch due to brief service failure. • Limited effect on the outcomes and/or objectives of more than one business unit. • Staff work hours are increased by less than 15% (6 hours per week) for less than two weeks. • Less than a 1% increase in staff turnover in a six-month period that can be directly attributed to the risk eventuating.	• Impact can be managed within current resources, with some re-planning. • Increase of between 5% and 7% in yearly operating costs. • One time financial cost between $10,000 and $20,000.
1	**Minimal**	• Reputation is not affected. • No questions from the Minister. • No media attention. • All communications and recovery can be managed internally.	• No loss or significant threat to health or life. • The agency's safety practices are questioned but are found to be appropriate.	• Limited effect on the outcomes and/or objectives of a business unit. • Staff work hours are increased by less than 5% (1 - 2 hours per week) for less than seven days. • No increase in staff turnover as a result of the risk eventuating.	• Impact can be managed within current resources, with no re-planning. • Increase of less than 5% in yearly operating costs. • One time financial cost of less than $10,000.

Rating

	Almost never	Possible but unlikely	Possible	Highly probable	Almost certain
Severe impact	15 Zone 3	19 Zone 3	22 Zone 4	24 Zone 4	25 Zone 4
Significant impact	10 Zone 2	14 Zone 3	18 Zone 3	21 Zone 3	23 Zone 4
Moderate impact	6 Zone 2	9 Zone 2	13 Zone 2	17 Zone 3	20 Zone 3
Minor impact	3 Zone 1	5 Zone 2	8 Zone 2	12 Zone 2	16 Zone 3
Minimal impact	1 Zone 1	2 Zone 1	4 Zone 2	7 Zone 2	11 Zone 2

To think about

- This can be specific to YOUR business
- You might only deal with thousands of dollars
- You might have much more of a focus on people’s safety
- Reputation might mean the world to you
- Being available might be critical to your survival

Recommendation 1

- It is recommended that the code is reviewed, and updated to implement input validation. Code should then be peer reviewed, and put through a static analysis tool before testing in production.

- It is recommended that logging is implemented and alerting conducted when SQL injection type attacks are conducted.

- Secure developer training should be regularly conducted to ensure that developers are aware of secure coding techniques and to ensure that they are reducing the likelihood for vulnerabilities to be introduced in the code.

Recommendation 2

- Implement a WAF

Recommendation 3

- Do nothing

It’s your choice

- What you do is up to you and the business
- You can’t always go with the elegant solution due to $$, time, technical constraints etc.
- Risk is a mechanism to show what an issue might cause, to what and why that’s a bad thing

Summary so far

- What the issue is
- What the associated risk is
- What causes the risk
- What this risk leads to
- How bad the risk is
- What we can do to fix this

Example 2

- You’ve just acquired a company - lots of problems to fix but…
- Privilege escalation bug in website xyz
- Can allow a user to get global admin
- Need to know a specific set of parameters to modify - so likelihood is possible
- Impact is major - has the ability to take over other users accounts
- Hasn’t been realised yet, so not yet an issue

Example 2

- “Hi CxO. We’re not validating requests correctly on the login page to the xyz website, mainly due to bad validation. Bla bla bla bla bla. The websites fundamentally broken and we need to take it down for weeks to get this working properly”

Example 2

- Huh?
- Why’s that bad?
- Do we really need to take it down?
- What will happen if we don’t?
- How much will this cost us if we don’t/ What will it cost us if we do?
- What else can we do?
- Will this solution fix every problem?

Example 2

- “Due to bad coding practices in legacy code, it is possible for a malicious person with a low privilege account to escalate privilege to an administrative account on the xyz website. This could allow information disclosure, modification or loss, or cause system outages”

- The likelihood is possible, as they would have to have some existing knowledge, but the impact is critical as they can access all data, delete other users accounts, and cause outages.

- We can put a WAF in place in the meantime to sort this out which will cost about $x; or

- We can remove admin functionality which will make users life more diffcult, but reduce the attack surface; or

- We can pull down the entire site and redevelop.

Food for thought

- Highlights alternatives to the ‘obvious’
- Are there better ways you can do something?
- Are there simpler ways you can do something?
- If I implement a control here - will that reduce multiple risks?
- Can this save me money?
- Is that high on a pen test report actually high risk? This processes ‘normalises’ severities to your own context

Summary

- Risk frameworks can aid you getting solutions to the issues that bug you most

- A well documented risk can highlight the issue as well as what it affects and leads to

- Risk can be a good way to normalise issues from external reports/ tools and ensure you have understood what is being put in front of you (think bug bounties)

- By presenting it in this way, it’s easily digestible by management and you’ll get money for the things you want

What not to do now

- Paperwork for paperworks sake - This doesn’t need to be a 100 page document - it could be a simple spreadsheet, series of JIRA tickets, whatever works in your org

- For ‘security’ to be tasked with doing this - Anyone in the org including developers, security teams, managers can do this, and it’s important to get everyone involved to get real value

- Spend all your money on getting someone with no context to do this for you - it’s worth having a look at your own environment first.

Useful Resources

- https://www.digital.govt.nz/dmsdocument/3-risk-assessment-process-information-security/

- https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/security/

- https://acsc.gov.au/infosec/mitigationstrategies.htm

- https://slack.engineering/moving-fast-and-securing-things-540e6c5ae58a

- https://www.cert.govt.nz/it-specialists/critical-controls/10-critical-controls/

Questions

- peter@quantumsecurity.co.nz
- @pjakowetz on twitter
- Come and have a chat afterwards in the foyer