NTNU

Norwegian University of Science and Technology

Photo by Allan Mas from Pexels

Risk management during development

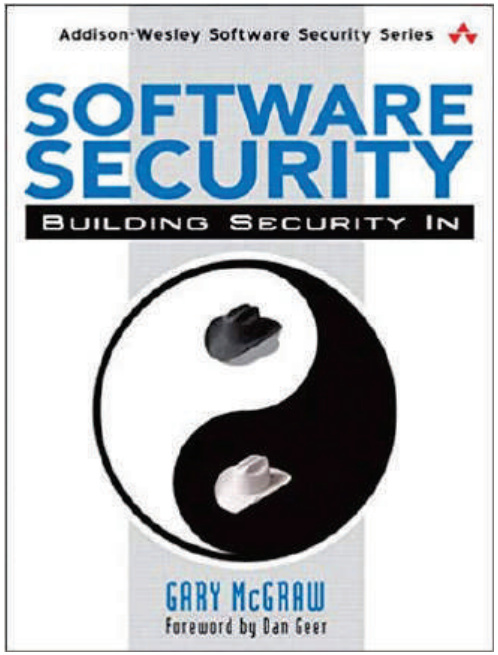
TDT 4237 2025

Per Håkon Meland

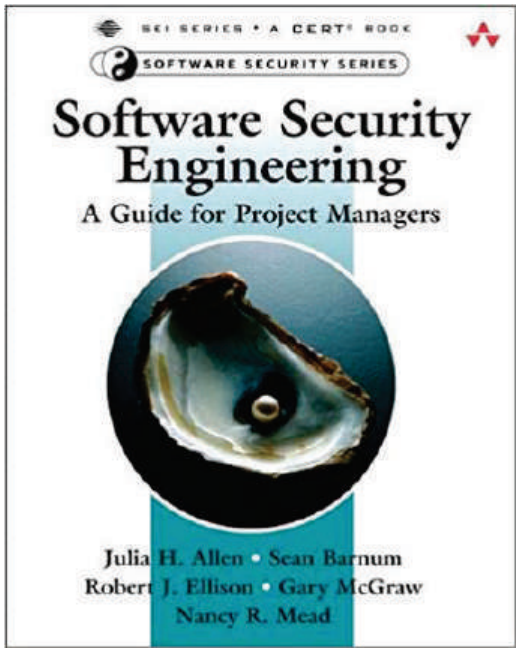
Agenda

- Risk Management Framework (RMF)
  - Security requirements
- Risk quantification
  - Security economics
  - Common Vulnerability Scoring System (CVSS)

Risk Management Framework (RMF)



2006



2008

https://www.garymcgraw.com/wp-content/uploads/2015/11/bsi3-risk.pdf

NTNU

enisa

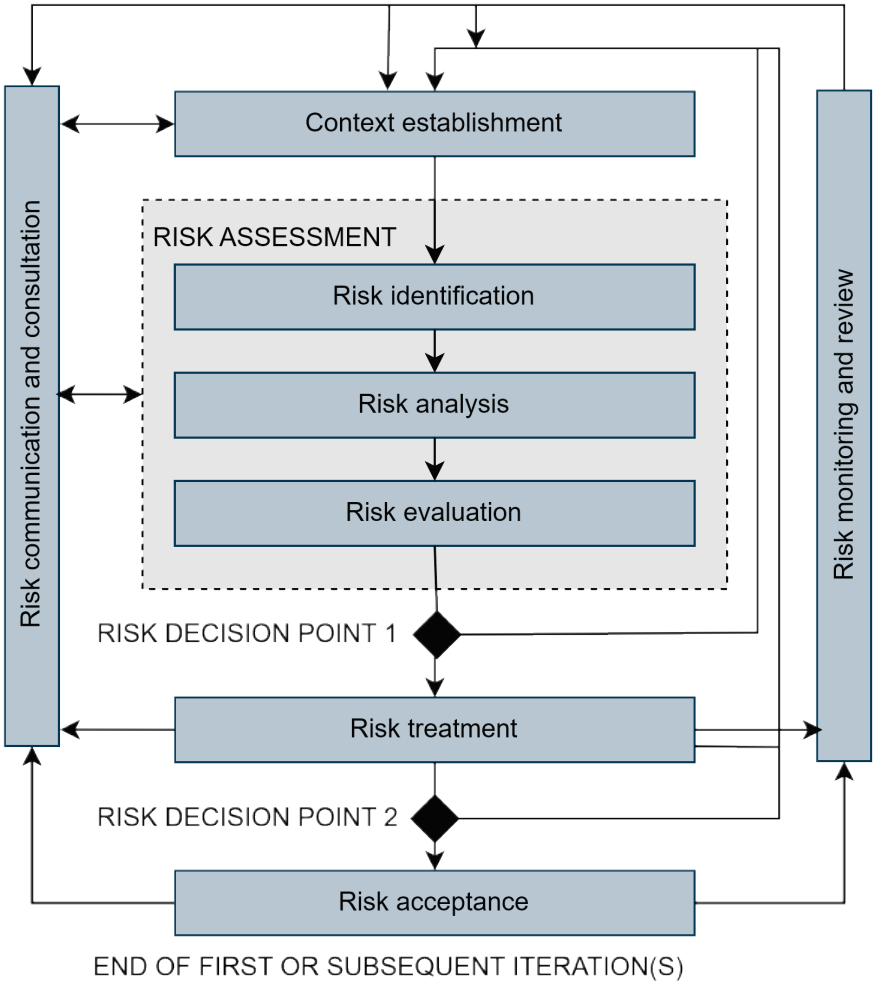
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

COMPENDIUM OF RISK MANAGEMENT FRAMEWORKS WITH POTENTIAL INTEROPERABILITY

Supplement to the Interoperable EU Risk Management Framework Report

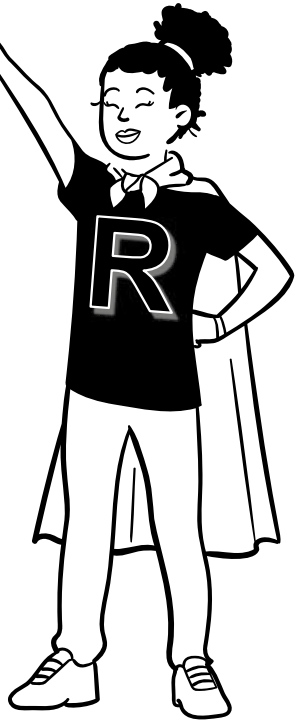
JANUARY 2022

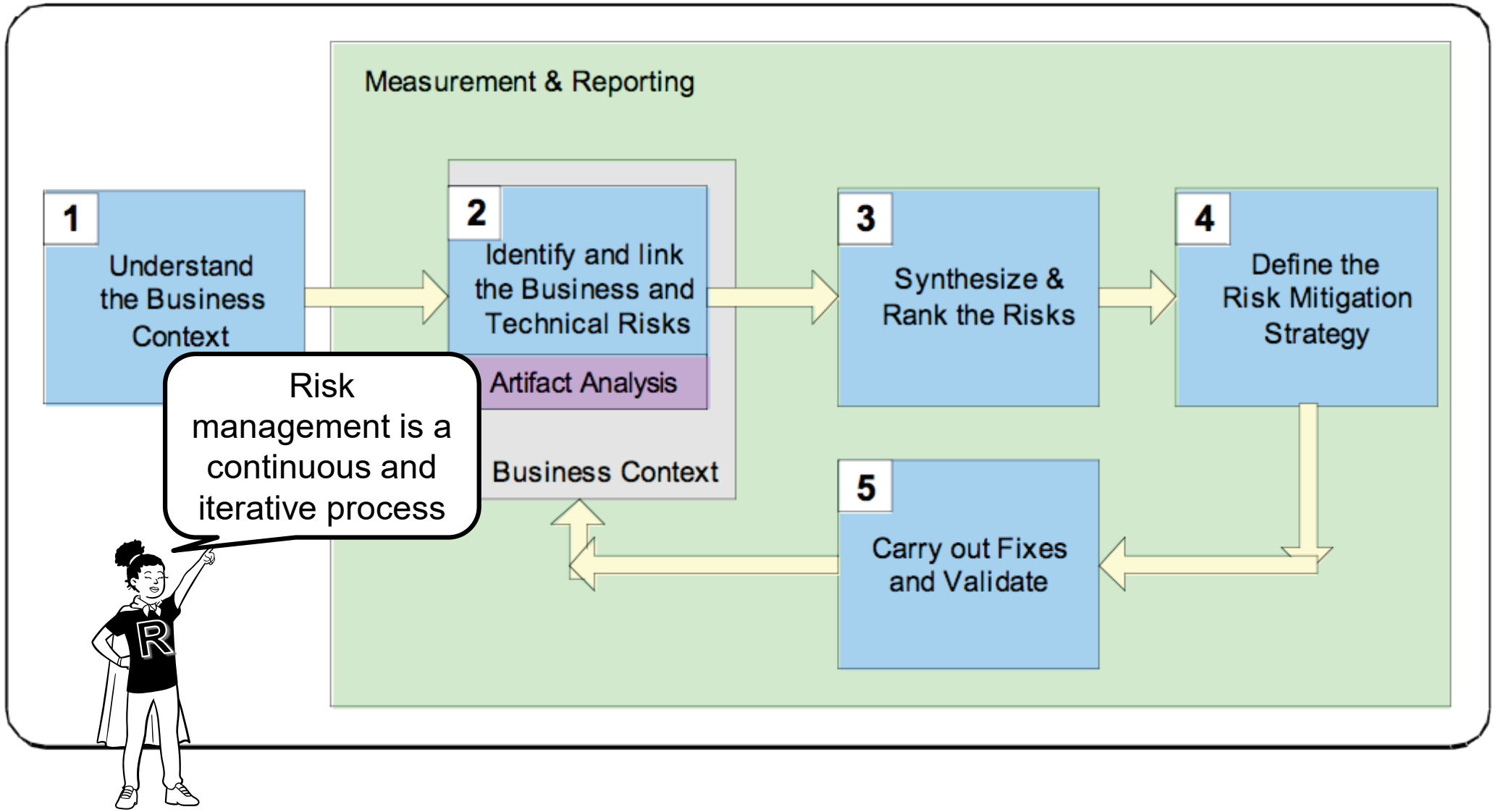
ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks



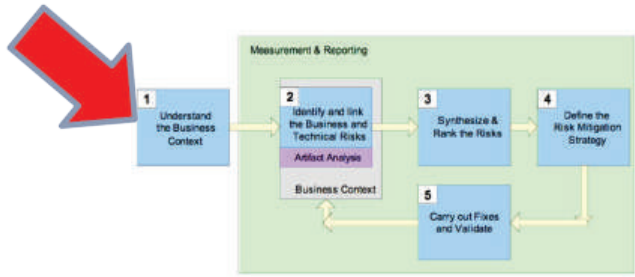
NTNU

Basic idea: identify, rank, track, and understand software security risk as it changes over time.



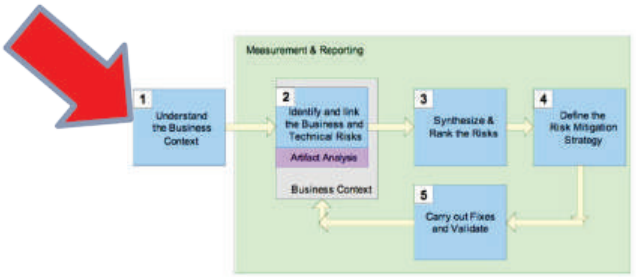

Measurement & Reporting
1
Understand the Business Context
2
Identify and link the Business and Technical Risks
Artifact Analysis
Business Context
3
Synthesize & Rank the Risks
4
Define the Risk Mitigation Strategy
5
Carry out Fixes and Validate
Risk management is a continuous and iterative process
R

1. Understanding the business context



- Business goals
  - Circumstances to care about
  - Risk scales (Impact and likelihood)
- (Business) assets - What are you trying to protect?
- Stakeholders
  - Users, regulators, attackers, etc.

1. Understanding the business context (cont')



- Business goal examples
  - Increase revenue by 27%
  - Meeting the service level agreements 98% of the time
  - Reducing development costs by 2%
  - Reducing operational costs by 4 million bucks annually
  - High return on investment (>2%)
  - Provide values to the society
  - Receive positive user satisfaction ratings above 80%
  - Etc.

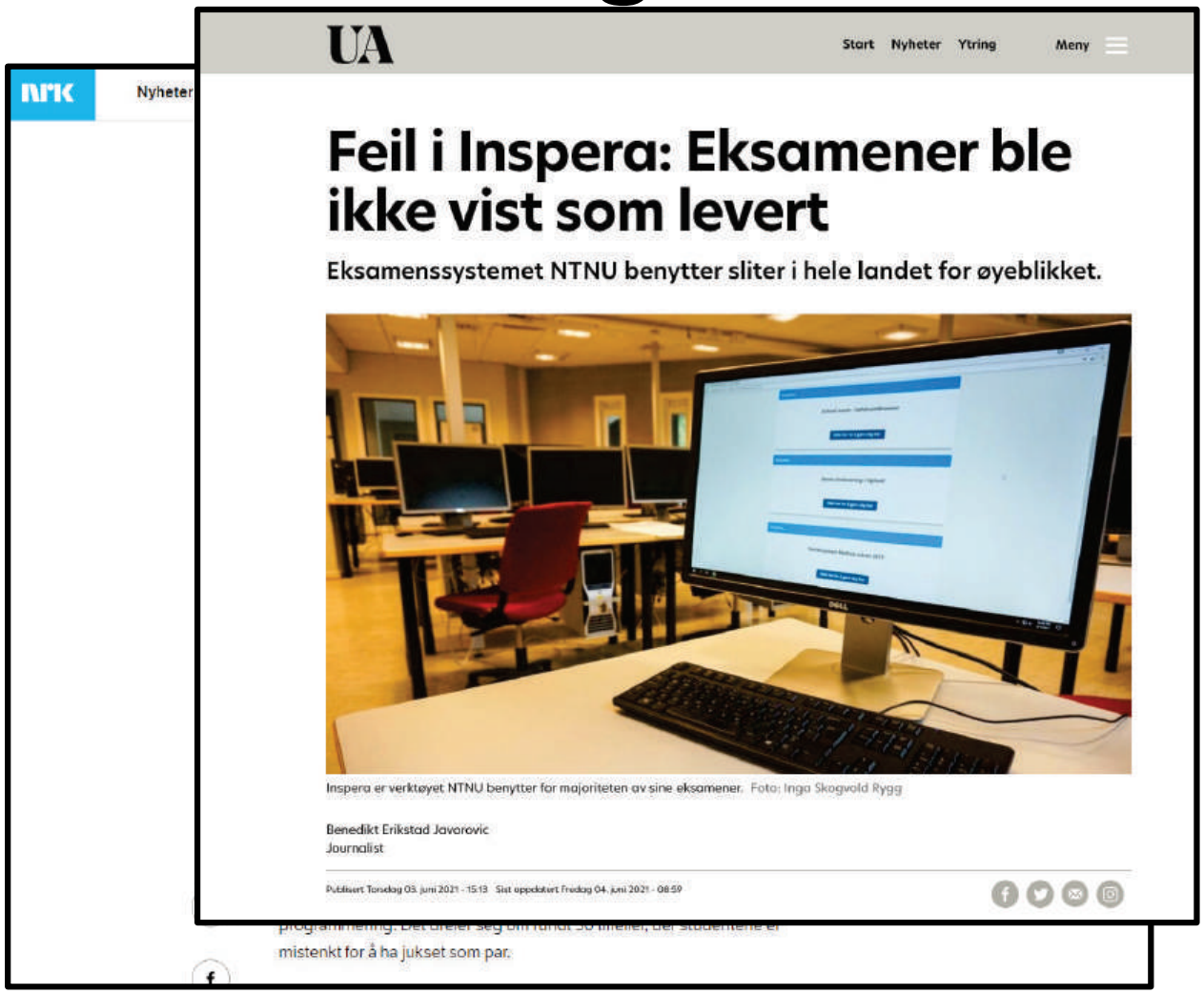
Example: Digital exams

Image: Jönköping University

- **Exams are created, solved and graded online**
- **Personal computers**
- **Confined room (or at home)**
- **Actors:**
  - **Professors, TAs, external examinators**
  - **Student(s)**
  - **Software developers, administrators**

Business assets of the digital exam system

- Exam assignments
- Individual answers
- Grades
- Users
- University reputation



Examples of business goals for the digital exam system

BG1:	Create high quality exams
BG2:	Reduce cost and errors - less manual handling of answers
BG3:	Students can do online exams remotely with 99,9% availability
BG4:	Save ink by 99%
BG5:	Trustworthy exams

Risk dimensions and scales

- Likelihood
  - Attacker-centric (see threat modeling lecture)
  - Expected frequency

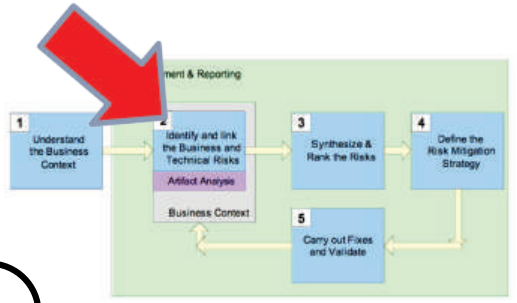
Low	Medium	High	Extreme
Once every 10 years or less	Once per year or less	Once per month or less	Every week

- Impact/consequence (next page)

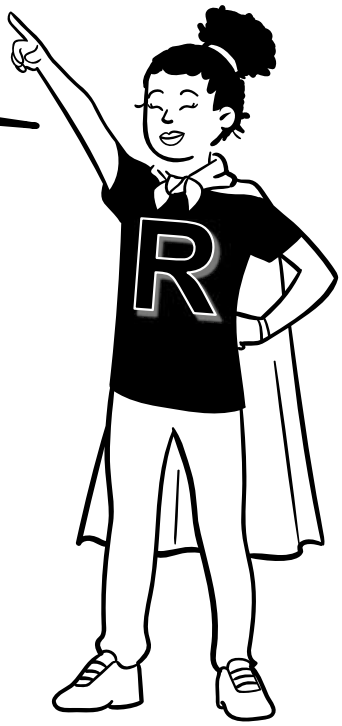
https://www.unit.no/aktuelt/hvordan-minimere-risiko-ved-digital-eksamen

Dimension	Low	Medium	High	Extreme
Confidentiality	No or minimal exposure of internal information or individual personal data.	Exposure of internal information or individual personal data.	Exposure of confidential information or sensitive or personal data of many.	Exposure of secret information or all personal data.
Availability	Tasks can be performed with delays or poorer quality.	Unsatisfactory quality or severe delays.	Limited ability to perform tasks.	Not possible to perform critical tasks.
Financial	Lesser economic loss that can be restored.	Significant economic loss that can be restored.	Irreperable economic loss	Significant and irreperable economic loss
Reputation	No loss of reputation and little influence on trust.	Reputation and trust can be damanged.	Damage to repuatation, serious loss of trust.	Serious damage to reputation and trust.

2. Identify business risks

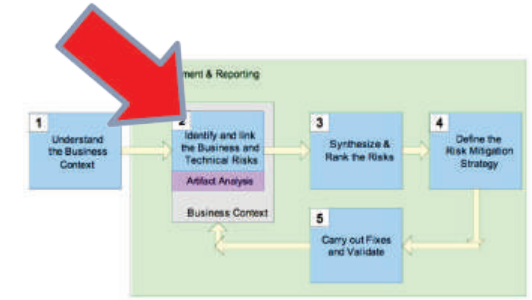


Business risks directly threaten one or more of a customer's business goals.



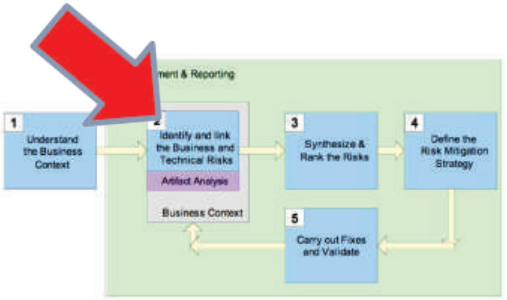
- Data – sensitive data stolen
- Time - processing delay
- Money - can’t make sales, can’t process transactions
- Reputation and brand - loss of trust
- Legal - compliance, contractual regulation

Examples of business risks to the digital exam system



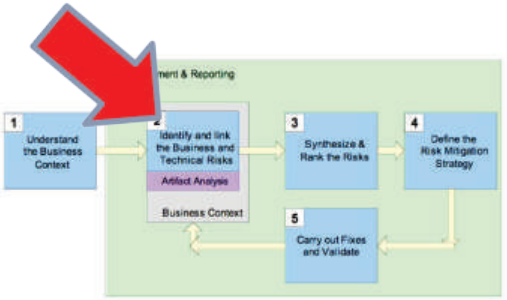
BR1: System too difficult to use (unnecessary mistakes)
BR2: System unavailable (unable to do deliver answers)
BR3: User identity is disclosed (legal penalty)
BR4: Individual answers are disclosed (legal penalty)
BR5: Automatic checking fails (incorrect grades)
BR6: Exam assignments leaked (retake exams)
BR7: Results cannot be trusted (wrong grades)
BR8: Too expensive to implement the system (more costly than paper exams)

2. Identify technical risks and link them with business risks



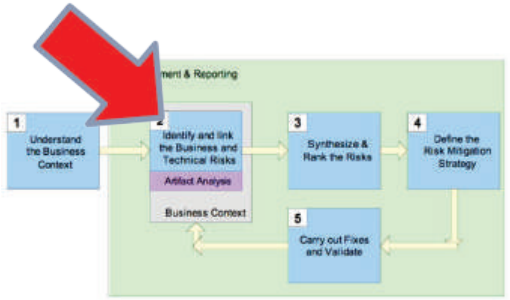
- Technical risks
  - Various threats and attacks that may bring negative impacts on business
- Inputs to identify technical risks could be:
  - Documents: System design, requirements, code
  - User feedback, interviews, discussions
  - Testing
  - Threat intelligence
- Tools to help identify technical risks
  - Misuse cases, attack trees, data flow diagrams, etc.

Example of technical risks



ID	Technical risks
TR1	Network jammed by DOS attack
TR2	Web server crashes under attack
TR3	Attacker types in wrong password several times to lock user accounts
TR4	Session hijacking is used to access answers of other students
TR5	Laptop can communicate with parallel network
TR6	SQL injection attacks against database
TR7	Safe exam browser runs in virtual machine
TR8	A student can login to several accounts at once

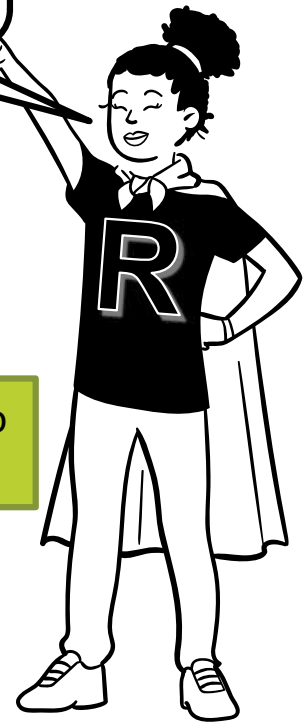
Linking



BG2: Reduce cost and errors

BG5: Trustworthy exams

Traceability!



BR3: User identity is disclosed

BR5: Automatic checking fails

BR7: Results can not be trusted

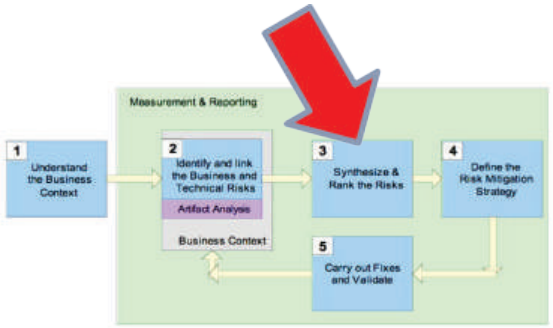
TR6: SQL injection attacks against database

TR4: Session hijacking is used to access answers of other students

TR8: A student can login to several accounts at once

TR7: Safe exam browser runs in virtual machine

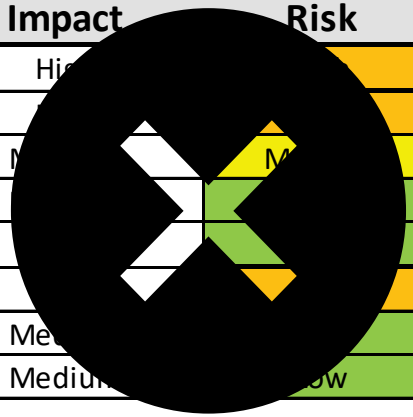
3. Synthesize and prioritize Risks

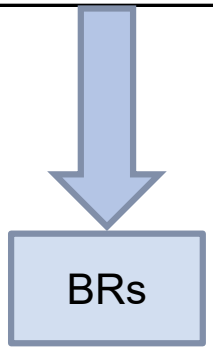


Impact \ Likelihood	Low	Medium	High	Extreme
Low	L	L	M	H
Medium	L	M	H	H
High	M	H	H	E
Extreme	H	H	E	E

Ranking of technical risks

ID	Technical risks	Likelihood	Impact	Risk
TR1	Network jammed by DOS attack	Medium	Hi	
TR2	Web server crashes under attack	Medium		
TR3	Attacker types in wrong password several times to lock user accounts	Medium	M	M
TR4	Session hijacking is used to access answers of other students	Low		
TR5	Laptop can communicate with parallel network	Low		
TR6	SQL injection attacks against database	High		
TR7	Safe exam browser runs in virtual machine	Low	Me	
TR8	A student can login to several accounts at once	Low	Mediu	ow



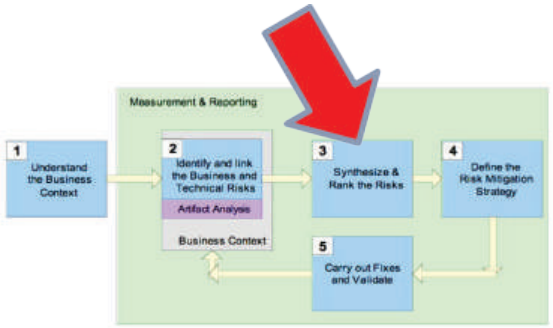


Ranking of business risks

Exposure of confidential information (Impact high)
Irreperable economic loss (Impact high)
Damage to reputation (Impact high)

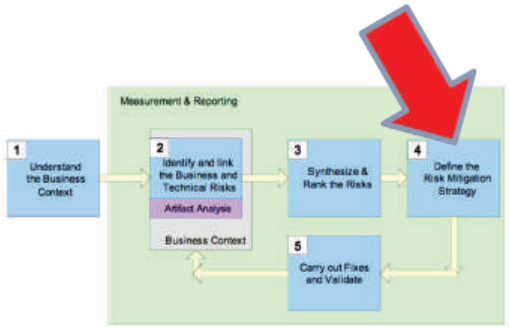
Business risks	Likelihood	Impact	Risk
BR1: System too difficult to use (unnecessary mistakes)	High	High	High
BR2: System unavailable (unable to do deliver answers)	Medium	High	High
BR3: User identity is disclosed (legal penalty)	Low	High	Medium
BR4: Individual answers are disclosed (legal penalty)	Low	High	Medium
BR5: Automatic checking fails (incorrect grades)	Low	Medium	Low
BR6: Exam assignments leaked (retake exams)	Low	High	Medium
BR7: Results can not be trusted (wrong grades)	Low	High	Medium
BR8: Too expensive to implement the system (more costly than paper exams)	Medium	High	High

Present risks



Impact \ Likelihood	Low	Medium	High	Extreme
Low				
Medium	BR5			
High	BR3, BR4, BR6, BR7	BR2, BR8	BR1	
Extreme				

4. Define the risk mitigation strategy



- Reducing the likelihood of the risk
- Reducing the severity of risk impacts
- Derive security requirements

*A **security requirement** is a statement of needed security functionality that ensures one of many different security properties of software is being satisfied.*

OWASP®

Examples of security requirements

Technical risks	Security requirements
TR3: Attacker types in wrong password several times to lock user accounts	Two-factor authentication should be required. Logs should contain source and results of login attempts.
TR6: SQL injection attacks against database	User inputs should always be validated and sanitized.

Criteria for good requirements

- What you require, not how to achieve it
  - Being open to different solutions
  - Avoid premature design or implementation decisions
- Understandability, clarity (not ambiguous)
- Cohesion (one thing per requirement)
- Testability
  - Clear acceptance criteria
  - Often requires quantification

Donald G. Firesmith

Firesmith, D. (2003). Engineering security requirements. *J. Object Technol.*, *2*(1), 53-68.
Tøndel, I. A., Jaatun, M. G., & Meland, P. H. (2008). Security requirements for the rest of us: A survey. *IEEE software*, *25*(1), 20-27.

Security requirement examples

- Bad ones
  - The system shall encrypt all confidential data using the RSA algorithm
  - Be secure
  - There should be no vulnerabilities in the code
  - The Web-server should log all access attempts and users should have unique identifiers
  - There could be password hashing in the user database table
- Better ones
  - The upload / download of customer data should be encrypted
  - The encryption keys must be generated by a specified party (provider/customer/3rd party)

The OWASP Application Security Verification Standard (ASVS)

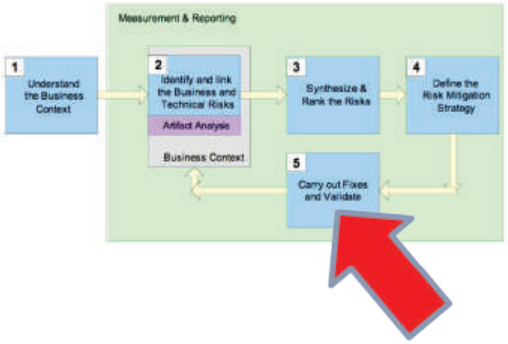
- A catalogue of available security requirements and verification criteria

V2.5 Credential Recovery

#	Description	L1	L2	L3	CWE	NIST §
2.5.1	Verify that a system generated initial activation or recovery secret is not sent in clear text to the user. (C6)	✓	✓	✓	640	5.1.1.2
2.5.2	Verify password hints or knowledge-based authentication (so-called "secret questions") are not present.	✓	✓	✓	640	5.1.1.2
2.5.3	Verify password credential recovery does not reveal the current password in any way. (C6)	✓	✓	✓	640	5.1.1.2

https://owasp.org/www-project-application-security-verification-standard/

5. Carry out fixes and validate

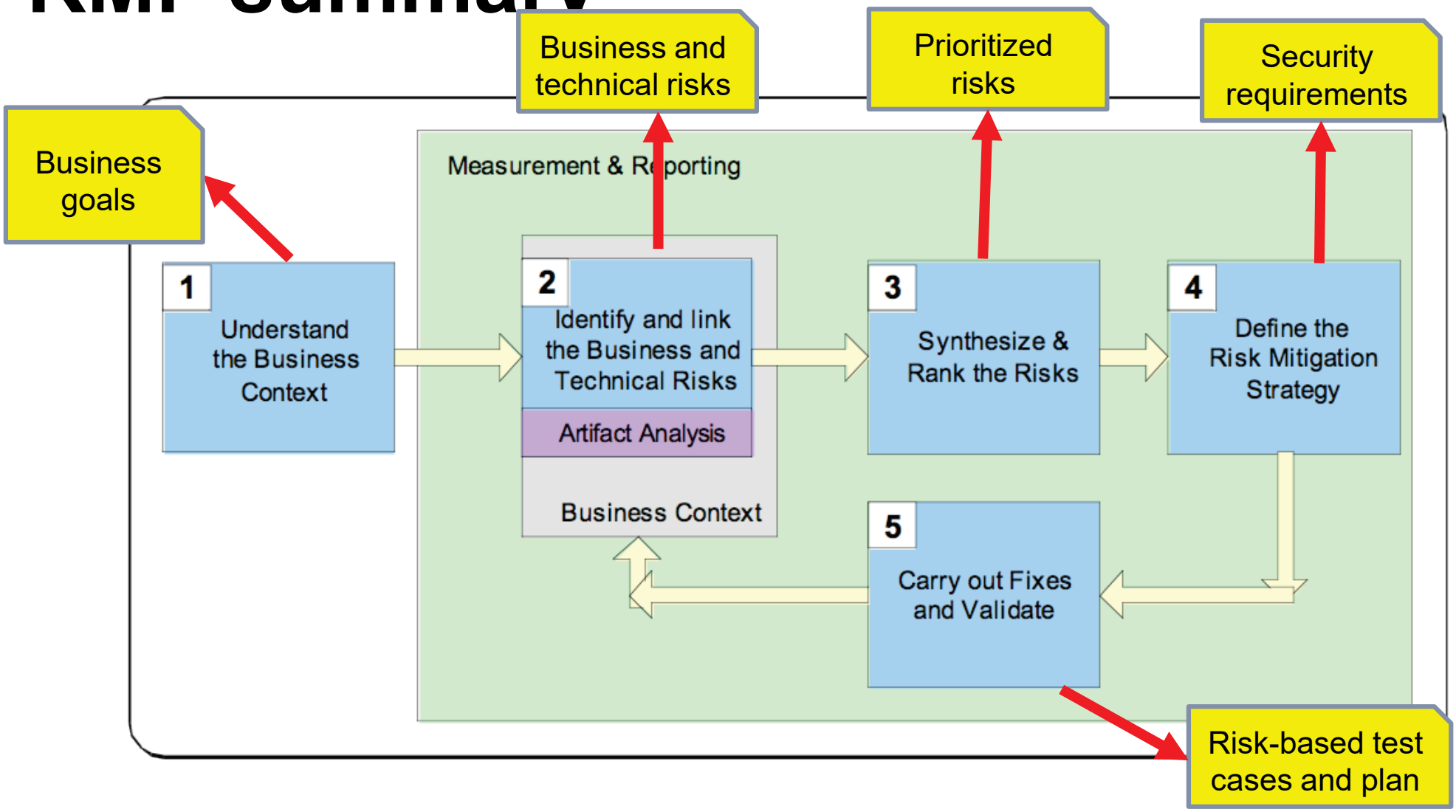


- Fixes
  - Implementation of mitigation strategies
- Validate
  - Risk-based testing (risk mitigated?)
    - Focusing on security requirements
    - Make test plan to test security requirements
    - Link test cases with technical risks/requirements
    - Prioritize test cases by risks (and costs)

Example of a test plan

Related risk	Test Case ID	Test priority (1-3)	Test description
User inputs should always be validated and sanitized.	TC6.1	2	Check if OR 1=1 possible on login
	TC6.2	2	Insert metacharacters in query
	TC6.3	1	Automated tests - fuzzing
	TC6.4	1	Static code analysis

RMF summary

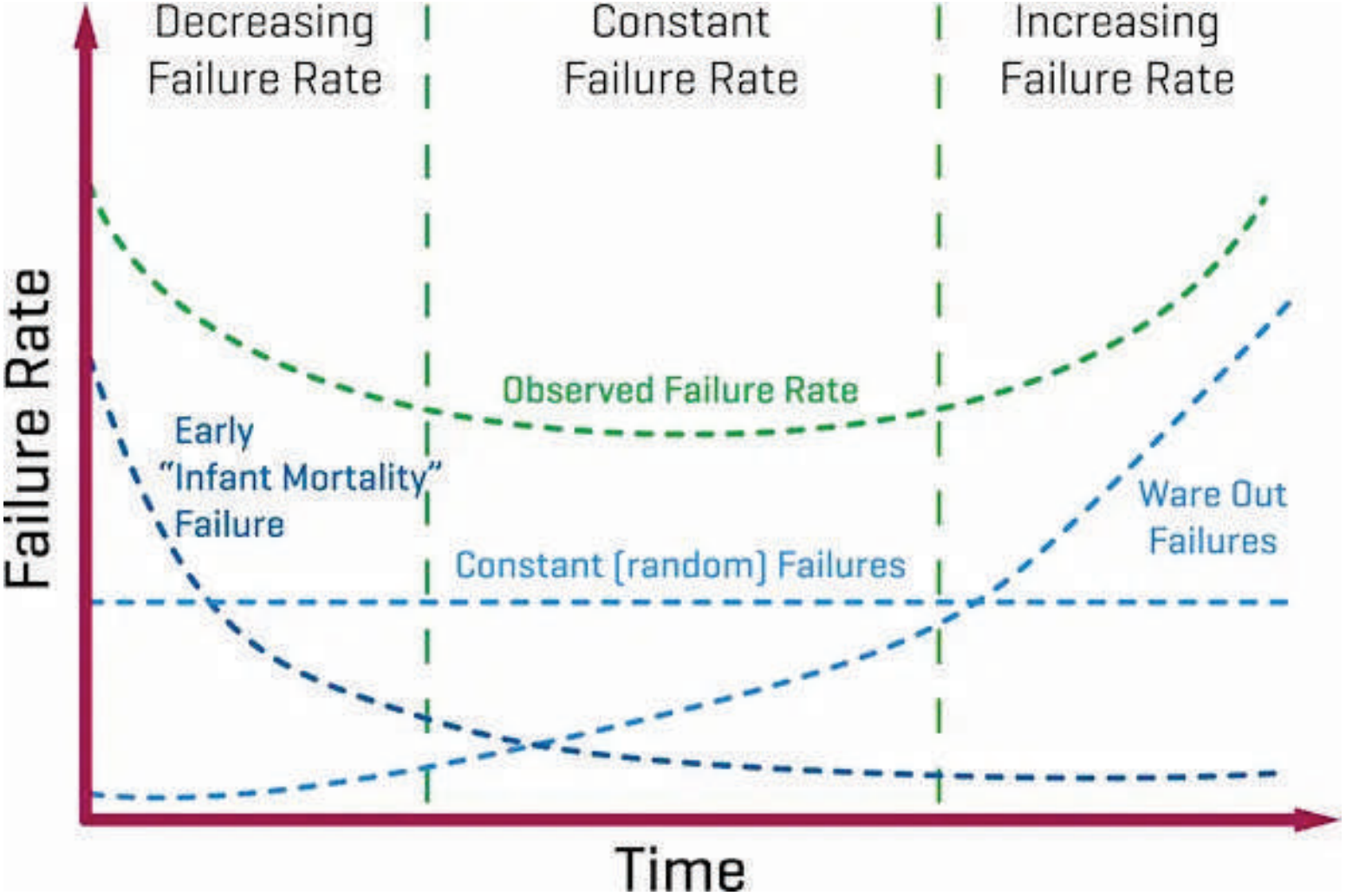

Business and technical risks
Prioritized risks
Security requirements
Business goals
Measurement & Reporting
1
Understand the Business Context
2
Identify and link the Business and Technical Risks
Artifact Analysis
Business Context
3
Synthesize & Rank the Risks
4
Define the Risk Mitigation Strategy
5
Carry out Fixes and Validate
Risk-based test cases and plan

Let’s try…

Business Goal 6: Avoid exam cheating

www.menti.com

Risk quantification

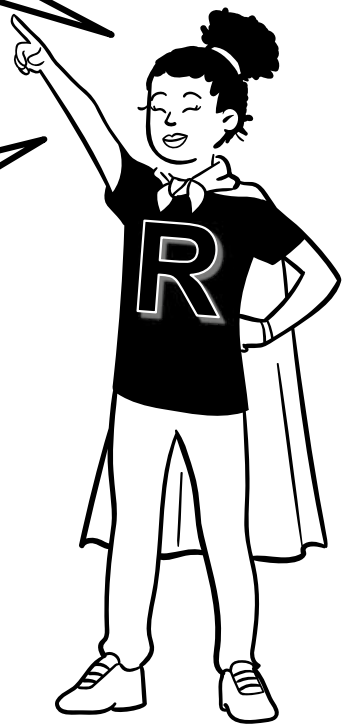


Source: https://passive-components.eu/reliability-and-mtbf-we-think-we-know-what-we-mean-but-do-we/

NTNU

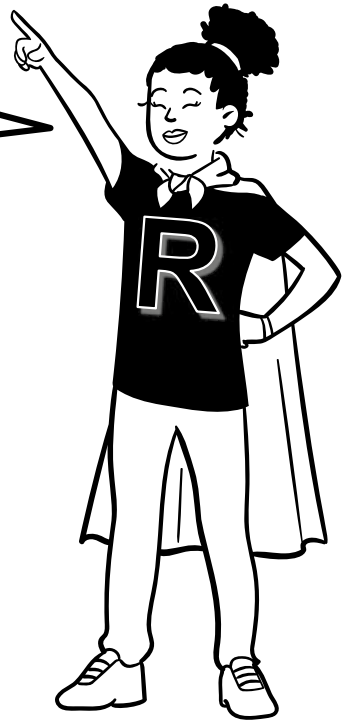
Safety deals with the effects of random failure

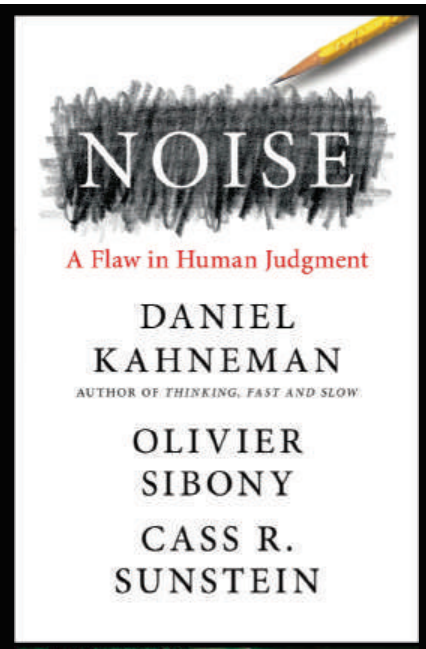
In security we assume a **hostile** opponent who can cause some of the components of our system to fail at the **least convenient** time and in the **most damaging** way possible

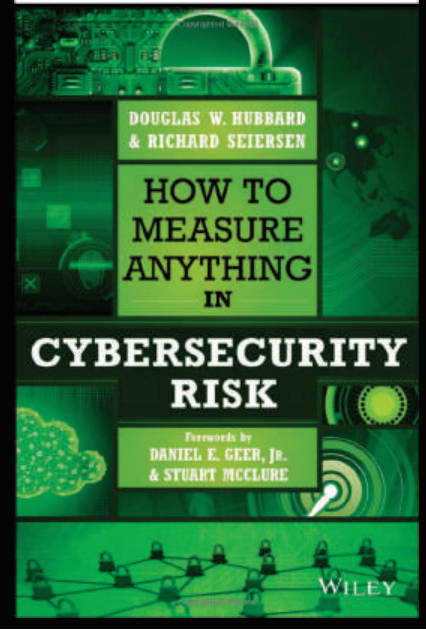


NTNU

Data like attack frequency, attack type distribution, number of successful attacks, number of prevented attacks and loss per attack are often not available.



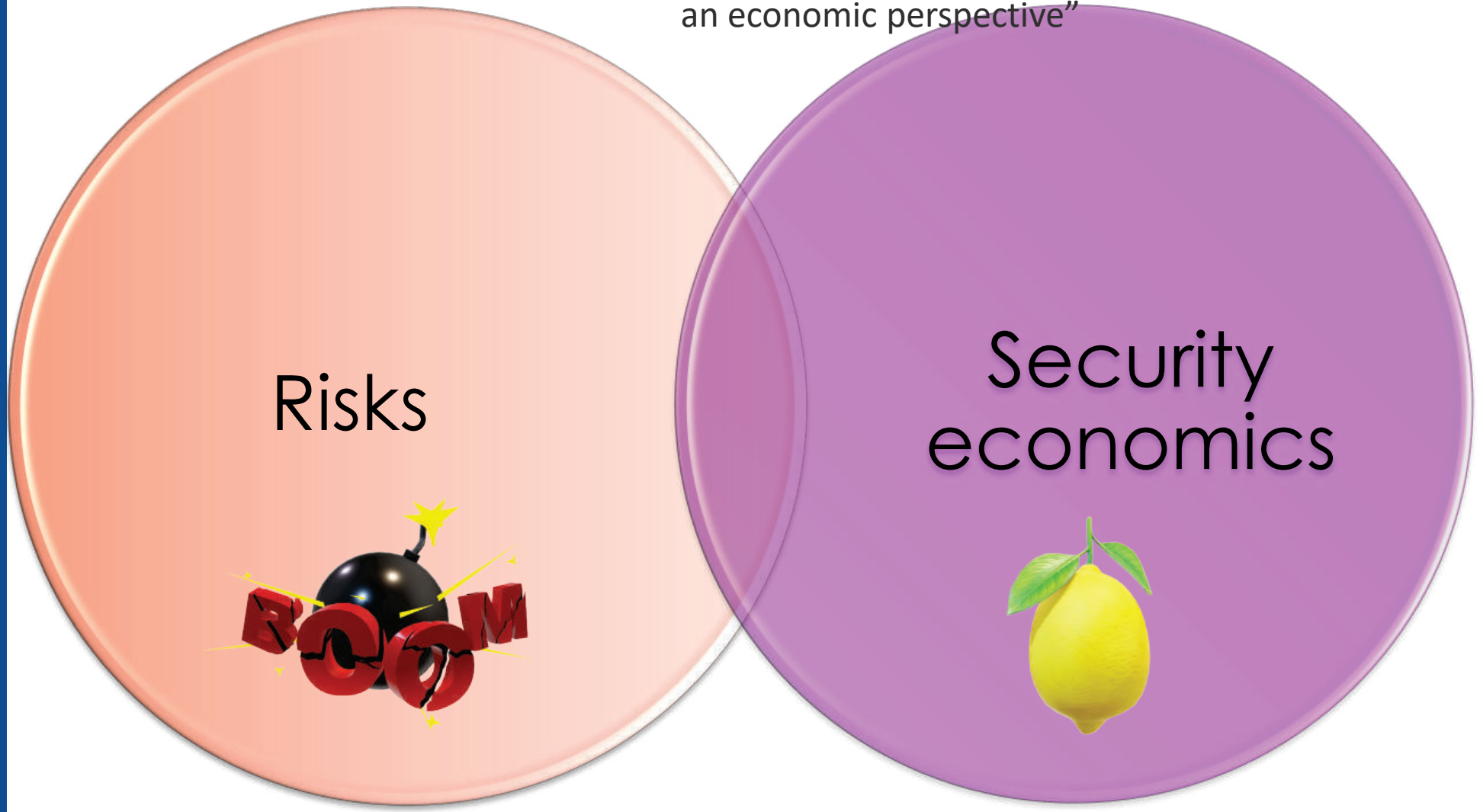


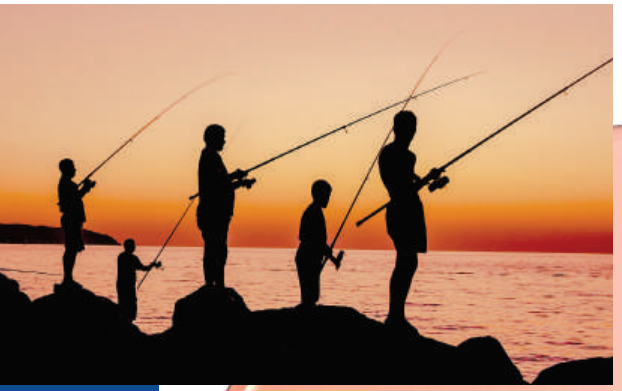


90% certain estimates …

… wrong 65% of the time

R. Anderson (2001): “Why information security is hard – an economic perspective”





Risks

Security economics

Schechter & Smith (2003): “Economic threat models”

Defender investment

Defender reactive cost

Defender loss

Defender reimbursement

Source: Meland, P. H. (2021): “Storyless cyber security: Modelling threats with economic incentives”

Defender investment

Defender reactive cost

Defender loss

Defender reimbursement

Attacker investment

Attacker penalty

Attacker profit

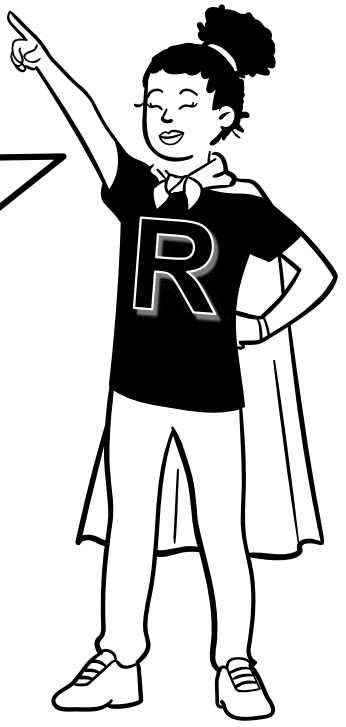
Attacker supplier profit

Attacker opportunity cost

Source: Meland, P. H. (2021): “Storyless cyber security: Modelling threats with economic incentives”

Possible sources:

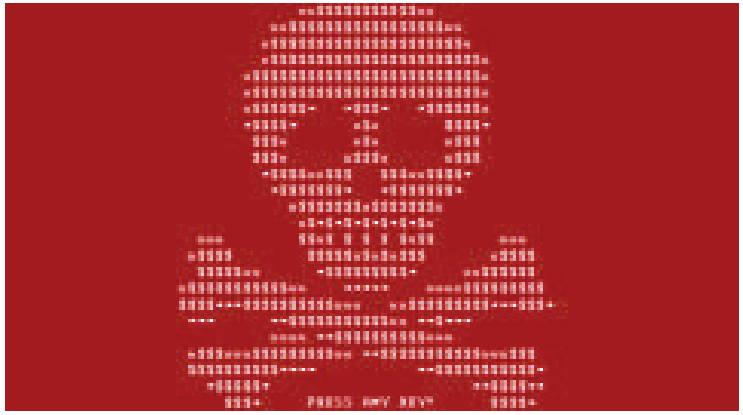
- Expert/specialist opinions,
- cyber loss events,
- coverage estimations,
- incident claims,
- retail price lists,
- dark net markets,
- coin crypto market cap,
- profit simulations,
- …



Example: Cryptojacking

"…in the latter part of 2017, it (cryptojacking) overshadowed almost all other malware threats"

Example: Ransomware



"I think that the reason [ransomware] is proliferating – we've seen twice as many attacks this year as last year in the UK – is because it works. It just pays."

Jeremy Fleming

The head of the UK spy agency GCHQ

Example: Attack outsourcing

Category	Product	Avg. Dark Web Price (USD)
Social Media	Hacked Facebook account	$65
	Instagram followers x 1000	$5
	Twitter retweets x 1000	$25
Hacked Services	Netflix 4K 1 year	$4
Email Database Dumps	Private USA dentists database 122k	$50
DDOS Attacks	Unprotected website, 10-50k requests per second, 1 hour	$15
	Unprotected website, 10-50k requests per second, 1 week	$500
	Premium protected website, 20-50k requests per second, multiple elite proxies, 24 hours	$200

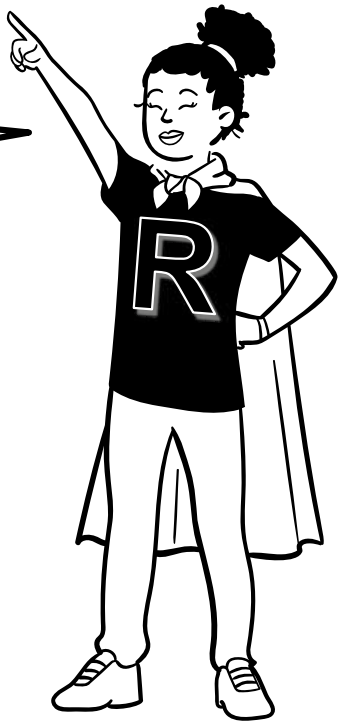
Source: Dark Web Price Index 2021

Let’s try…

Spending!

Defender’s dilemma

Breaches are inevitable because defenders have to be right 100% of the time whereas attackers only have to be right once



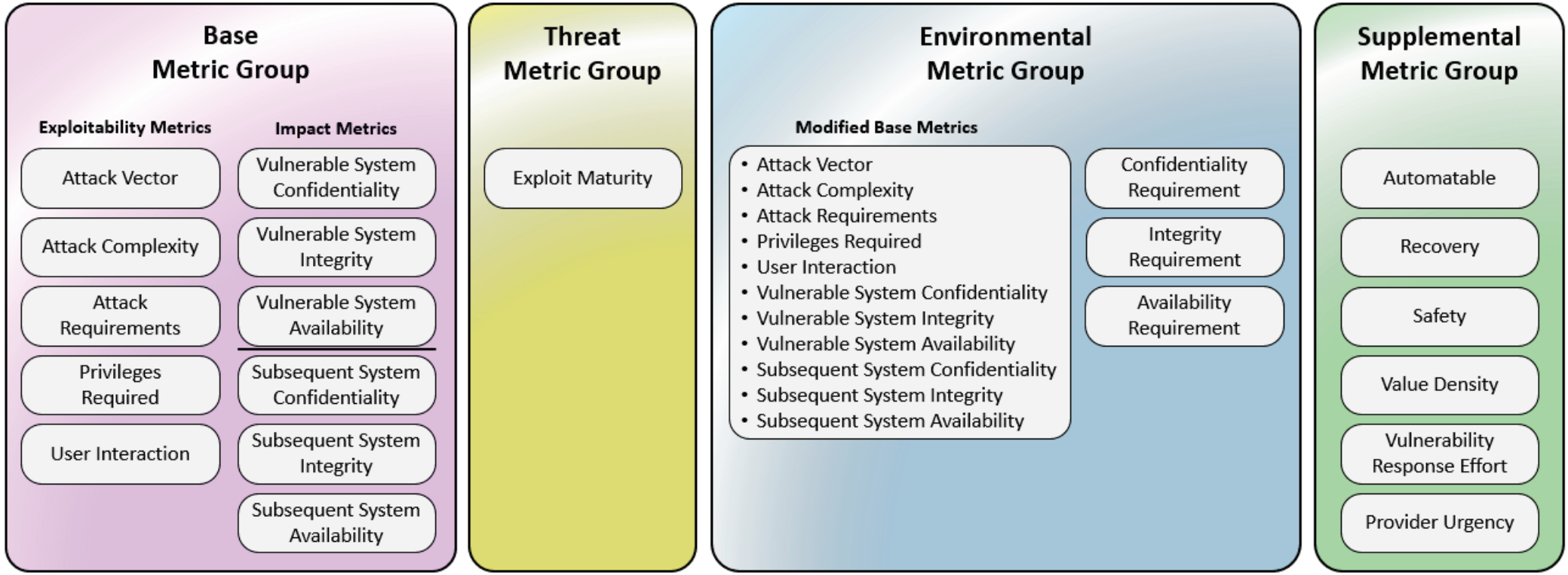
NTNU

Common Vulnerability Scoring System

https://www.first.org/cvss/

- A standardized way of measuring the technical severity of a vulnerability
- Gives a score between 0-10
- Consists of a:
  - Base: constant over time and across user environments
  - Threat: characteristics of a vulnerability that change over time
  - Environmental: unique to a user's environment
  - Supplemental: do not modify the final score, gives additional insight

- Not a direct risk value by itself (CVSS != Risk)
- A high CVSS does not necessarily mean a high risk likelihood



Source: https://www.first.org/cvss/v4.0/specification-document

NTNU

Let's try…

Goto:
https://www.first.org/cvss/calculator/4.0

Derive a score for the following scenario:

After login in to Inspera, you find out that you can manipulate the URL to change the user ID and get read access to exercises of other students.

Bonus example

An issue was discovered in the Calendar feature in Zimbra Collaboration Suite 8.8.x before 8.8.15 patch 30 (update 1), as exploited in the wild starting in December 2021. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document.

NTNU

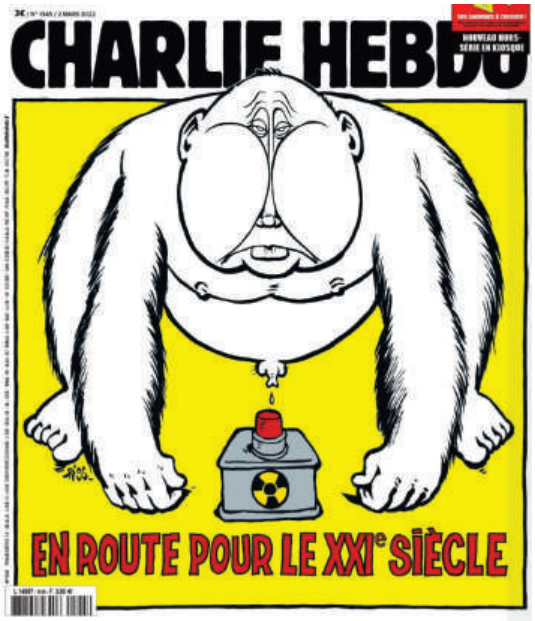
CVSS v4 Score: Base 5.1

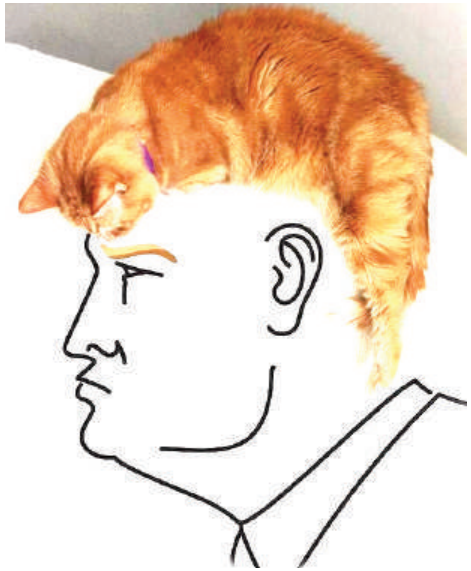
Metric	Value	Comments
Attack Vector	Network	The vulnerable system is accessible from remote networks.
Attack Complexity	Low	No specialized conditions or advanced knowledge are required.
Attack Requirements	None	No attack requirements are present.
Privileges Required	None	No privileges are required for an attacker to successfully exploit the vulnerability.
User Interaction	Active	A targeted user must click a malicious link that is provided by an attacker.
Vulnerable System Confidentiality	None	There is no direct impact to the web application confidentiality.
Vulnerable System Integrity	None	There is no direct impact to the web application integrity.
Vulnerable System Availability	None	There is no direct impact to the web application availability.
Subsequent System Confidentiality	Low	An attacker could read data from the user's browser.
Subsequent System Integrity	Low	An attacker could modify data in the user's browser.
Subsequent System Availability	None	There is no direct availability impact to the user's browser.

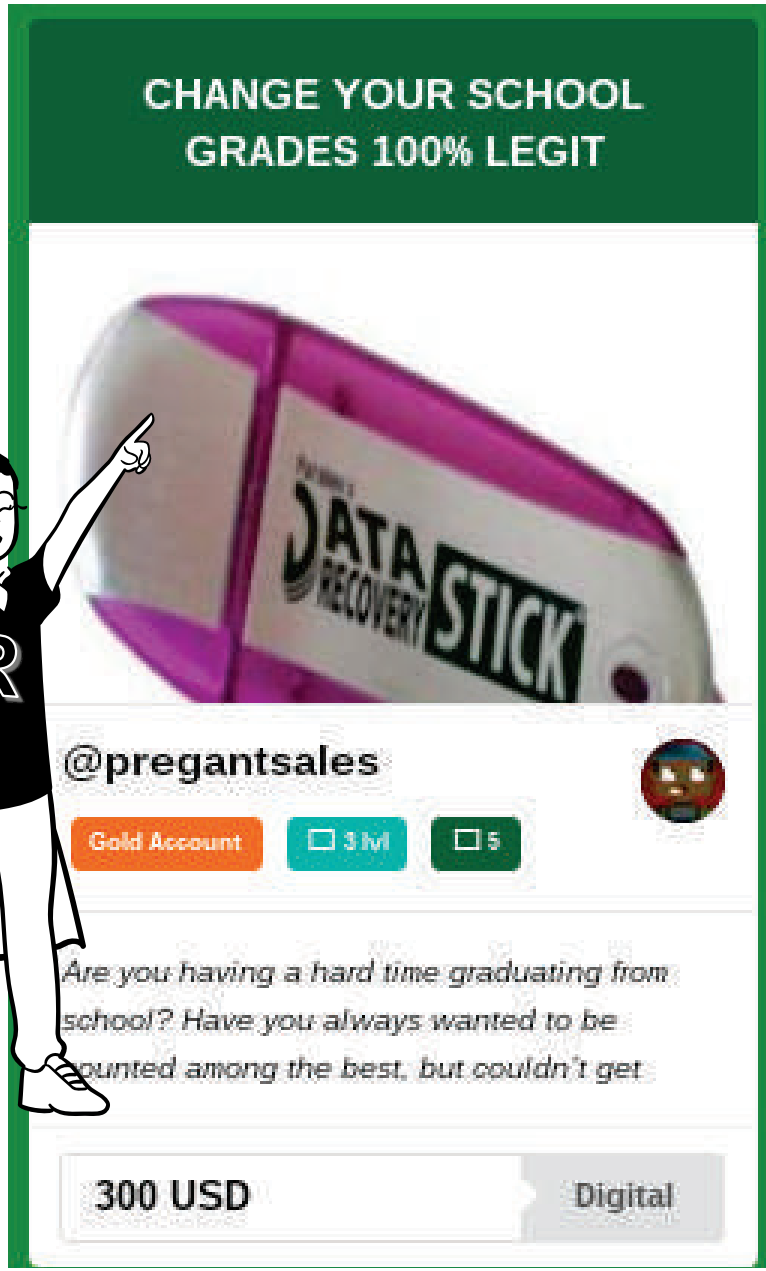
Summary

- Security is about risk management
- Use a systematic and sensible approach
- Security is a game of economics

…. but beware of irrational attackers!







NTNU

Next time!

Static Analysis and Tools for Security

Pen Testing for Web Applications