Security Administration

Let’s get down to business

Agenda

- Cybersecurity Framework
  - Building security into a business
- Risk Assessment
  - Building our understanding
- Incident Handling
  - Building a security strategy
- General Data Protection Regulation
  - Adopting rules
- IAM
  - Managing access

Cybersecurity Framework

Set of best practices, guidelines & standards for managing cybersecurity risk to critical infrastructure

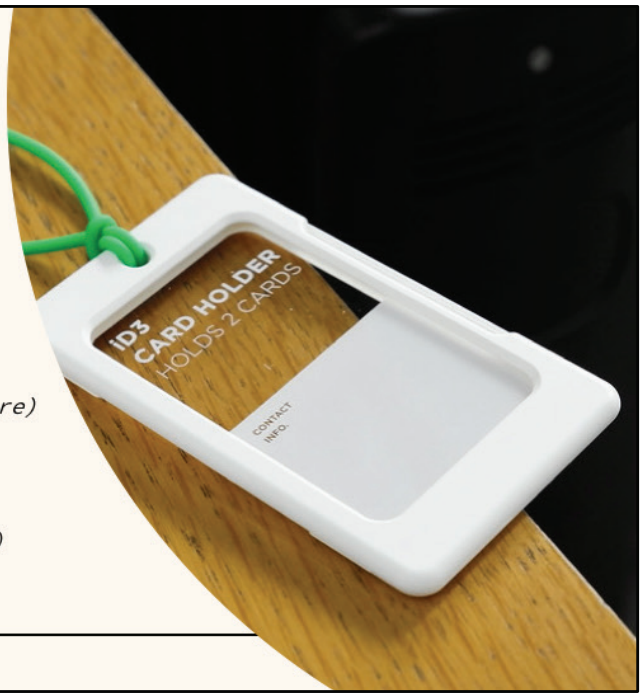
NIST Cybersecurity Framework v1.1

Security 360

Credit: N. Hanacek/NIST
https://www.nist.gov/cyberframework

Identify

- Lay framework foundations
- Understanding the risk to
  - Systems *(connected infrastructure)*
  - Assets *(items of value)*
  - People *(employee & client)*
  - Data
  - Capabilities *(skills, controls)*



Security 360

Protect & Detect

- Protection
  - Develop & implement safeguards to protect
    - Access control
    - Awareness Training
    - Maintenance

- Detection
  - Develop & implement activities to identify events
    - Network monitoring
    - Anomalies

Respond & Recover

- Response
  - Develop & implement actions to take during an event
    - Analysis
    - Mitigation
- Recovery
  - Develop & implement actions to take after an event
    - Improvements
    - Communication

Security 360


Risk Assessment
Security 360

Risk Management

- Good risk management establishes a strategy to:
  - Assess
  - Respond
  - Monitor

- Strong relation to the framework
  - Assess is a big part of **Identify**
  - Respond is a big part of **Respond**
  - Monitor is a big part of **Detect, Respond & Recovery**

Defining Risk

- Threats
  : Event negatively impacting organisation
- Vulnerabilities
  : Known weaknesses
- Harm
  : Possible damage, the impact
- Likelihood
  : Probability of occurence

Calculating Risk

- A complex function of the

likelihood that a
threat will exploit a
vulnerability and the magnitude of
harm it may cause

- Risk aggregation
  - Many smaller calculated risks are combined to create a larger calculated risk

Security 360

Sounds like we need a strategy

- A strategy involves the *entire* organisation
  - CEO, CTO, CS Management, CS responders, staff

Different players, different responsibilities:

Policies (Top Management)
- Lay out the rules

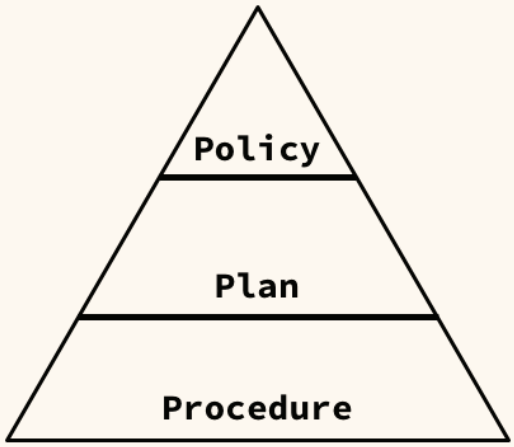
Plans (CS Management)
- How to implement the rules conceptually

Procedures (CS Responders, Staff)
- What to do to satisfy the rules practically

Strategize

General & broad

Detailed & specific



Security 360

Policies

- The highest level
- Definitions
  - What an incident is
  - Who is responsible
  - Who has authority
  - Who should be informed
- Severity & Prioritisation
- Measures of Performance
- Reporting templates

Factors Affecting Policy

- Organisational
  - Values, stakeholders, mission
- Legal
  - Laws, regulations to observe
- Ethical
  - Being good
- Environmental
  - Community, sustainability, cultural
- **Risk Assessment**

Security 360

Policy-Making

- Common Policies
  - Computer security, standard security, acceptable use
- Common definitions
  - Event - an observation in an information system
  - Adverse Events - a negative **event**
  - Incident - **adverse event** which breaks a policy
  - Breach - **incident** resulting in release of data
- Common priorities
  - Incidents are prioritised over adverse events
  - Breaches are prioritised over incidents

Plans

- The next level down
- A bit more specific
  - What is the goal
  - Who responds
  - What resources are needed
  - How to communicate
- Which metrics to report

relates to a specific policy

Incident **Response** Planning

- Common goals
  - Protect data
  - Stop the attack
  - Keep the system up
- Common responders
  - On-call response team
- Common resources
  - Overtime
- Common communication
  - Emails sent to all

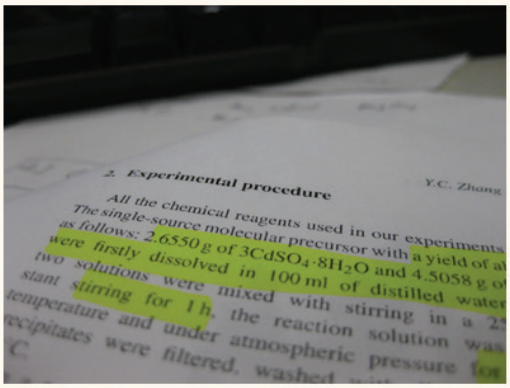
Incident **Recovery** Planning

- Common goals
  - Analyse the situation
  - Restore systems
  - Prevent another incident
- Common responders
  - Blue team
- Common resources
  - Planned maintenance (downtime)
- Common communication
  - Staff website posting

(Standard Operating) Procedures

- The lowest level
- Processes
  - Techniques
  - Calls
  - Checklists
  - Forms
- Guidelines
- Configuration

relates to the plan (goal)



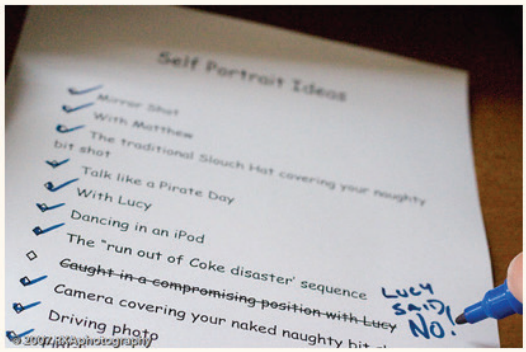
Security 360

Incident **Response** Procedures

- Sample Checklist (check & record)
  - ☐ Detect incident
  - ☐ Call on-call team
  - ☐ Determine level of severity
  - ☐ (high-severity) call in team / notify management
  - ☐ Analyse logs/IDS/IPS
  - ☐ Confirm entry vector
  - ☐ Contain attack
  - ☐ Mitigate attack

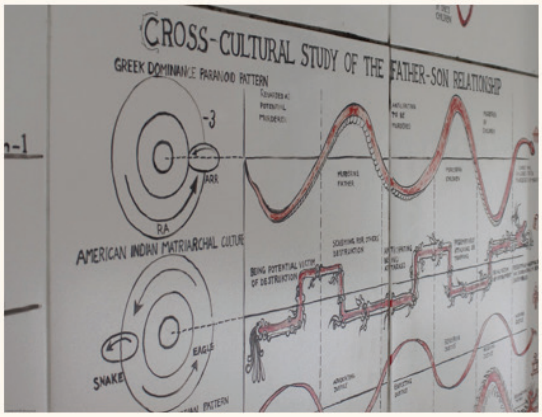
Incident **Recovery** Procedures

- Sample Checklist
  - ☐ Secure entry vector
  - ☐ Tighten network security
  - ☐ Scan systems
  - ☐ Patch systems
  - ☐ Restore systems
  - ☐ Collect analysis data
  - ☐ Prepare report



Analyse Response & Recovery

- Get the measures
  - Time attack starts
  - Time attack ends
  - Time of responder arrival
  - Time service down
  - Time service up
- Get the metrics
  - Attack length
  - Responder delay
  - Service downtime



Measure is a single “unit measurement”
Metric is the calculation using two measures

Re-evaluate

- Do the procedures need to change?
  - This is likely
  - Can we learn from the last attack and improve?
- Do the plans need to change?
  - This is possible
  - Was the plan lacking/in-conflict with procedures?
- Does the policy need to change?
  - This is unlikely

Security 360

Identify, Protect, Detect

Strategies for rest of the NIST Cybersecurity Framework

Maybe expand our policies

- Define
  - Assets - data/clients
  - SLA - 99.99% uptime
- Prioritise
  - What's most important
- Measurements
  - What do we measure?

New plans (and new goals)

- **Identify** assets / threats to assets
  - Sensitive data / data loss
  - Client / failure to meet SLA
- **Protect** assets
  - Ensure confidentiality
  - Ensure availability
- **Detect** attacks
  - Watch for MitM/Crypto attacks
  - Watch for DoS attacks

Security 360

New procedures

- **Identify**
  - Inform infosec team of new arriving data
  - Inform infosec team of new contracts
- **Protect**
  - Implement full-disk encryption, manage keys
  - Implement DDoS protection in NGFW
- **Detect**
  - Implement MitM alerts in Snort, test regularly
  - Implement DoS alerts in Snort, test regularly

Data Protection

with the General Data Protection Regulation

General Data Protection Regulation

Rules for protecting the rights and freedoms of natural persons with regard to the processing and movement of their personal data

GDPR Art. 1

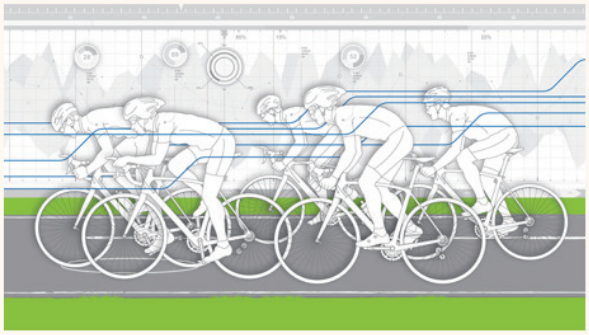
One law vs twenty-eight laws

Security 360

https://gdpr-info.eu/

Personal Data

- Name
- Address
- Location
- Online Identifier
- Health Info
- Income
- Culture
- Appearance
- and more...



Security 360

Data Players

- Data Subject
  - The “identifiable natural person”
  - The individual
- Data Controller
  - The entity holding the data
  - The organisation
- Data Processor
  - The entity processing the data
  - The service provider

Security 360

An Identifiable Natural Person

- Natural & living person
  - Not a business entity, corporation
- Directly or indirectly identifiable by:
  - Name
  - ID Numbers
  - Location
  - Online identifier

based on their personal data

Controller vs Processor

- Sometimes the same organisation
- Controlling
  - Making decisions about the data
  - Instructing the processor
- Processing
  - *collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*

Security 360

What's identifiable?

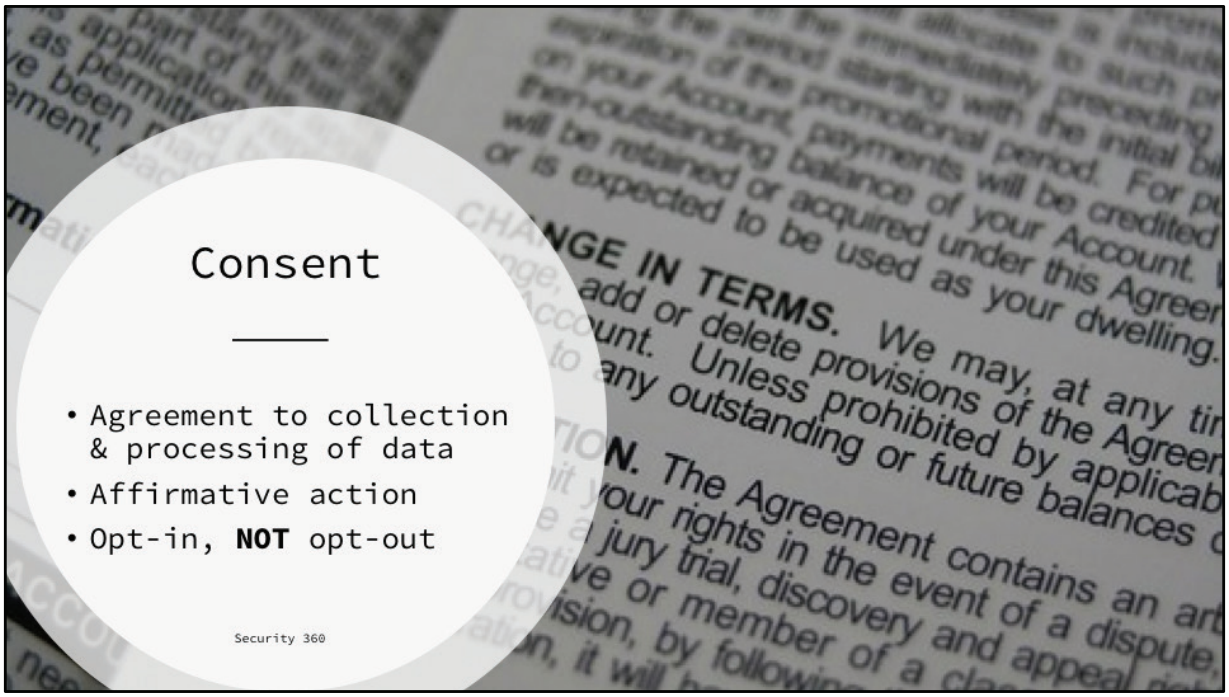
- Eg. our data set includes **ONLY** physical appearance
  - No names
  - No ID numbers
  - No locations
  - No online identifiers

- Do we have to comply with the GDPR?

Communicate

- Who is collecting & processing
- Why is it necessary
- How long will it be held

Security 360



Access & Portability

- The data subject can **get** their data
- The data subject can **move** their data

Security 360

Warn, Erase & Safeguard

- Warn
  - Incidents or breaches involving personal data
- Erase
  - If the data subject requests it
- Safeguard
  - Provide extra security for sensitive data (health, race, religion)

Data Protection Officer

- Not a cybersecurity role, but someone who works closely with the security team
- Assists with data compliance
- Mandatory for
  - Companies with operations relying on large personal data
  - Companies processing large personal data
  - Public authorities
- All organisations can voluntarily hire a DPO
  - If a DPO is not hired, staff take on data responsibility

Security 360

Policy-shift

- New regulations (like the GDPR) can affect policy
  - That then affects our lower layers
- More Planning
  - New plans to reflect how we cater to the policy updates
  - Eg. Ensure affirmative consent from our customers
- New Procedures
  - New processes to ensure we comply with the regulation
  - Eg. Provide a tick box during registration

Identity & Access

and their management (IAM)

Identity Management

- The **attributes** of a user
  - Something you know,
    Something you have,
    Something you are
  - Job Title
  - Project role
  - Department

Authenticating Identity

- Single-Factor / Multi-Factor
- Credential Management
  - Keep our passwords safe

Security Assertion Mark-up Language (SAML)
Digitally signed tokens for enabling:

Single Sign-On (SSO)
One organisation's resources

Federated Identity
Different enterprises' resources

Authorising Identity

- Access Management
  - Yes/no decisions for authorisation
- Active Directory
  - Authentication & authorisation

Security 360

Access Control

- Role-Based Access Control
  - Job title
    - Manager, red team, blue team
- Attribute-Based Access Control
  - Fine grain, lots of control
    - IF <attribute> AND <attribute> BUT NOT <case> THEN authenticate
- Rule-Based Access Control
  - FW rules, IDP rules
    - IP, Port, time of day
- Mandatory Access Control
  - Clearance levels
    - For example at The Pentagon