Cybersecurity and Business Continuity Training Day

Cybersecurity Primer & Best Practices

Peter Mayer

CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND

A few basics to get us all on the same page

Cybersecurity Protection Goals

- Originally only the C-I-A triad defined by NIST
  - **Confidentiality:** Ensuring that data or information is not made available or disclosed to unauthorized persons or processes.
  - **Integrity:** Guarding against improper information modification or destruction in an unauthorized and undetected manner.
  - **Availability:** Ensuring timely and reliable access to and use of information.

Cybersecurity Protection Goals

- Originally only the C-I-A triad defined by NIST
  - **Confidentiality:** Ensuring that data or information is not made available or disclosed to unauthorized persons or processes.
  - **Integrity:** Guarding against improper information modification or destruction in an unauthorized and undetected manner.
  - **Availability:** Ensuring timely and reliable access to and use of information.
- Two added by NIST later on
  - **Authenticity:** Verifying that a user, process, or device is the one claimed, often as a prerequisite to allowing access to resources in an information system.
  - **Non-repudiation:** Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Cybersecurity Protection Goals

- But there are even more, depends on the context
- They might contradict each other
  - E.g., encrypting data might increase confidentiality, but decreases availability
- Prioritisation of security goals depends on
  - **Assumptions** about the environment, actors, etc.
  - Risk analysis
- No system that is sufficiently complex to be practically useful is 100% secure
  - There are always bugs in the code
  - Side-channels to get secret info
  - …

Behavioural Economics

- Psychological factors greatly influence our decisions making
- Cybersecurity is no exception

- Imagine you had to decide between the following two options

A: Getting 500 DKK as a gift

B: Getting 1000 DKK as a gift with 50% chance

Behavioural Economics

- Psychological factors greatly influence our decisions making
- Cybersecurity is no exception

- Now imagine you had to decide between the following two

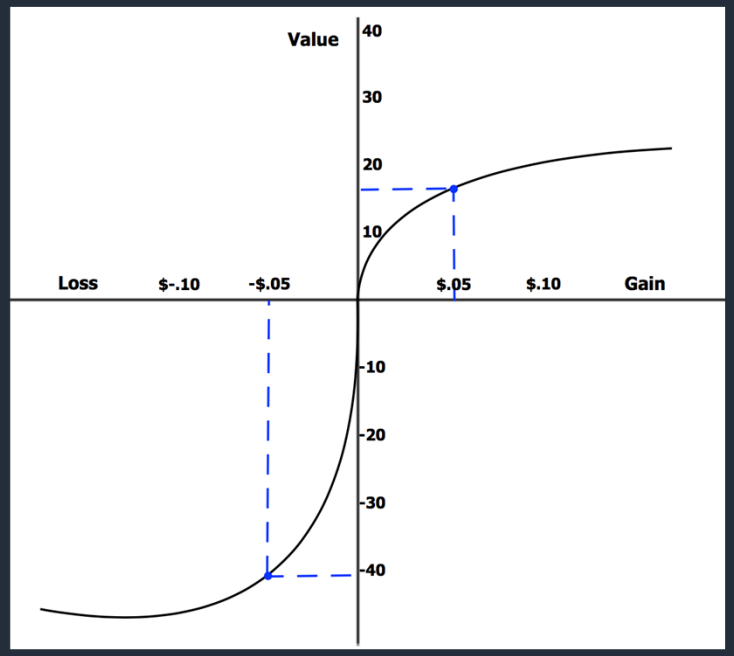
A: Having to pay 500 DKK as a fine

B: Having to pay 1000 DKK as a fine with a chance of 50%

Behavioural Economics

- Psychological factors greatly influence our decisions making
- Cybersecurity is no exception

- **Loss aversion:** We take more risks to avoid losses



Loss aversion and Cybersecurity

- How is this relevant in the context of cybersecurity?

- The scenario is not that different

A: Having to pay 500 DKK as a fine

B: Having to pay 1000 DKK as a fine with a chance of 50%

Loss aversion and Cybersecurity

- How is this relevant in the context of cybersecurity?

- The scenario is not that different

A: Having to pay 500000 DKK in security budget

B: Having to pay ??? DKK as recovery costs with a chance of ?? %

Insights & Best Practices for Good Cybersecurity

Awareness & Education Procedures Today

PCI Security Standards Council

Payment Card Industry
Data Security Standard

Requirements and Testing Procedures

Version 4.0.1

June 2024

PCI Security Standards Council

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Training of personnel ensures they receive the information about the importance of information security and that they understand their role in protecting the organization. Requiring an acknowledgment by personnel helps ensure that they have read and understood the security policies and procedures, and that they have made and will continue to make a commitment to comply with these policies. **Good Practice** Entities may incorporate new-hire training as part of the Human Resources onboarding process. Training should outline the security-related "dos" and "don'ts." Periodic refresher training reinforces key security processes and procedures that may be forgotten or bypassed. Entities should consider requiring security awareness training anytime personnel transfer into roles where they can impact the security of cardholder data and/or sensitive authentication data from roles where they did not have this impact. Methods and training content can vary, depending on personnel roles. **Examples** Different methods that can be used to provide security awareness and education include posters, letters, web-based training, in-person training, team meetings, and incentives. Personnel acknowledgments may be recorded in writing or electronically.
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	**12.6.3.a** Examine security awareness program records to verify that personnel attend security awareness training upon hire and at least once every 12 months. **12.6.3.b** Examine security awareness program materials to verify the program includes multiple methods of communicating awareness and educating personnel.	
	12.6.3.c Interview personnel to verify they have completed awareness training and are aware of their role in protecting cardholder data.	
Customized Approach Objective Personnel remain knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.	**12.6.3.d** Examine security awareness program materials and personnel acknowledgments to verify that personnel acknowledge at least once every 12 months that they have read and understand the information security policy and procedures.	

Awareness & Education Procedures Today

PCI Security Standards Council

Requirements and Testing	
Defined Approach Requirements	**Define**
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	**12.6.3.** record awaren every **12.6.3.** materi metho educat **12.6.3.** comple

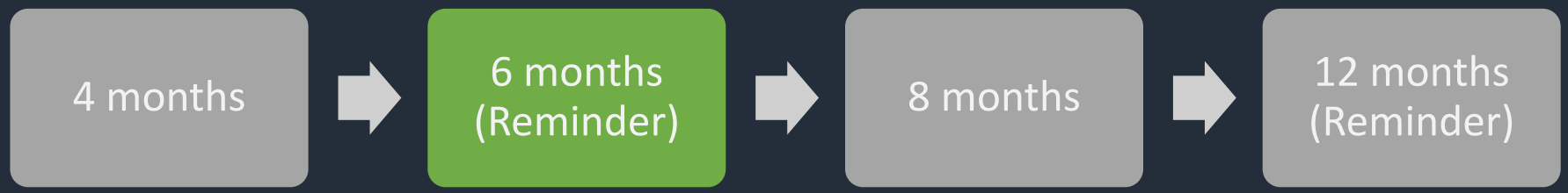
Are 12 months a good time frame to refresh?

- Longitudinal evaluation over 12 months
  - Evaluation of effectiveness after 4, 6, 8, 12 months
  - Reminder measures introduced after 6 months, re-tested after 12

4 months → 6 months (Reminder) → 8 months → 12 months (Reminder)

Are 12 months a good time frame to refresh?

- Longitudinal evaluation over 12 months
  - Evaluation of effectiveness after 4, 6, 8, 12 months
  - Reminder measures introduced after 6 months, re-tested after 12



Are 12 months a good time frame to refresh?

- Longitudinal evaluation over 12 months
  - Evaluation of effectiveness after 4, 6, 8, 12 months
  - Reminder me

4 month

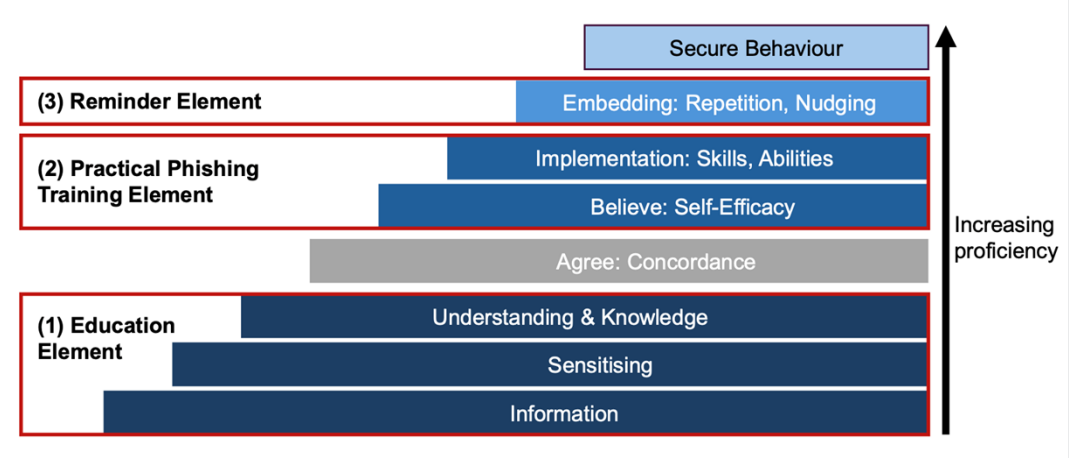
2 months
eminder)

No, cybersecurity knowledge and skills should be refreshed earlier!
Six months seems to be the best choice currently with a good measure in place.

Should everyone get the same measure/refresher?

- Investigation of personalised awareness & education measure
- Three groups divided according to their anti-phishing proficiency

- Personalisation of training seems promising in bridging proficiency gaps
- Participants with varying initial proficiency levels reached similar post-training proficiency levels

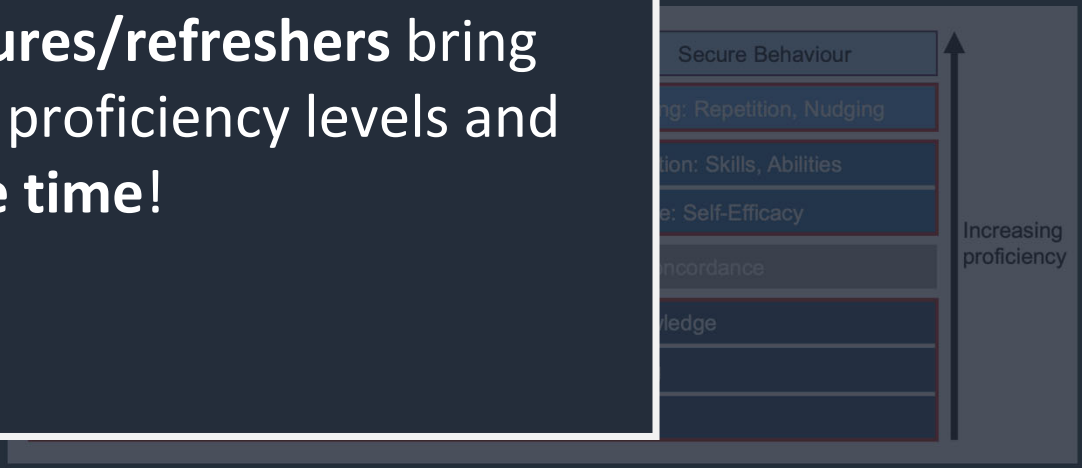


Should everyone get the same measure/refresher?

- Investigation of personalised awareness & education measure
- Three groups divided according to their anti-phishing proficiency

- Personalisati
  promising in
  gaps
- Participants w
  proficiency le
  post-training

No, tailored measures/refreshers bring people to the same proficiency levels and **save time**!



Can you use just any measure?

Commonly available security advice is of low quality

- Anti—phishing: lack of consistent, up to date anti-phishing information

Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector

Mattia Mossano
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany
mattia.mossano@kit.edu

Kami Vaniea
School of Informatics
University of Edinburgh
Edinburgh, United Kingdom
kvaniea@inf.ed.ac.uk

Lukas Aldag
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany
lukas.aldag@kit.edu

Reyhan Düzgün
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany

Peter Mayer
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany

Melanie Volkamer
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany

- Password: incomplete, contradicting

Vision: What Johnny learns about Password Security from Videos posted on YouTube

Mathieu Christmann
Technical University of Darmstadt
Darmstadt, Germany
mathieu.christmann@gmail.com

Peter Mayer
peter.mayer@kit.edu
SECUSO - Security, Usability, Society,
Karlsruhe Institute of Technology
Karlsruhe, Germany

Melanie Volkamer
melanie.volkamer@kit.edu
SECUSO - Security, Usability, Society,
Karlsruhe Institute of Technology
Karlsruhe, Germany

ABSTRACT
The text password is the most pervasive authentication scheme and is unlikely to disappear soon. Companies employ password

medium sized companies (SMEs) are likely to refer their employees to available material on the Internet.
Our research aims to analyse the quality of freely available videos

Evaluating Password Advice

Hazel Murray
Department of Mathematics and Statistics
Maynooth University, Ireland
Email: hazelmsmurray@gmail.com

David Malone
Hamilton Institute
Maynooth University, Ireland
E-mail: david.malone@nuim.ie

Can you use just any measure?

Commonly available security advice is of low quality

- Anti—phish
  information

- Password:

No, effective measures are of the essence! So ask before getting one.

Vision: What Johnny learns about Password Security from Videos posted on YouTube

Mathieu Christmann
Technical University of Darmstadt
Darmstadt, Germany
mathieu.christmann@gmail.com

Peter Mayer
peter.mayer@kit.edu
SECUSO - Security, Usability, Society,
Karlsruhe Institute of Technology
Karlsruhe, Germany

Melanie Volkamer
melanie.volkamer@kit.edu
SECUSO - Security, Usability, Society,
Karlsruhe Institute of Technology
Karlsruhe, Germany

ABSTRACT
The text password is the most pervasive authentication scheme and is unlikely to disappear soon. Companies employ password

medium sized companies (SMEs) are likely to refer their employees to available material on the Internet.
Our research aims to analyse the quality of freely available videos

Evaluating Password Advice

Hazel Murray
Department of Mathematics and Statistics
Maynooth University, Ireland
Email: hazelmsmurray@gmail.com

David Malone
Hamilton Institute
Maynooth University, Ireland
E-mail: david.malone@nuim.ie

Are mandatory password changes helpful?

- Password expiry is a trade-off between
- The **security lost** by forcing people to use coping strategies
  - People choose weaker passwords
  - Passwords are easy to guess based on previous one
- The **security gained** by giving the attacker a “moving target”
  - Prevents continued access for attacker who relies on password
  - Does not prevent continued access by backdoors, etc.

“In sum, these security-specific observations and the results […] suggest the security benefit of password aging policies are at best partial and minor.”

Are mandatory password changes helpful?

- Password expiry is trade-off between
- The secu
- The secu

No, regular password changes are discouraged by modern cybersecurity standards! The trade-off is not worth it. Instead, systems should be monitored and **users asked to change passwords only when a breach happened**.

The same is true for complexity rules by the way 😉

Brief Overview of Relevant Cybersecurity Frameworks & Standards

EU Network and Information Security (NIS) Directive

- EU-wide legislation aiming to increase common level of security across member states
- Current version: NIS 2
  - Came into effect on 17 October 2024
- Important change: companies are responsible for knowing if they are affected
- Effects on companies
  - Need to implement measures against cyber attacks
  - Non-compliance incurs substantial fees

EU Network and Information Security (NIS) Directive

Medium Sized Enterprises

- 50 – 250 employees
- Turnover of 10-50 million €
- Total assets <43 million €

Large Enterprises

- >250 employees
- Turnover of >50 million €
- Total assets >=43 million €

- But even some small enterprise (<50 employees) and microenterprises (<10 employees) are affected, e.g.,
  - DNS service providers
  - TLD name registries
  - Domain name registration services
  - Providers of public electronic communications networks
  - Public administration
  - Research (if deemed by state)

EU Network and Information Security (NIS) Directive

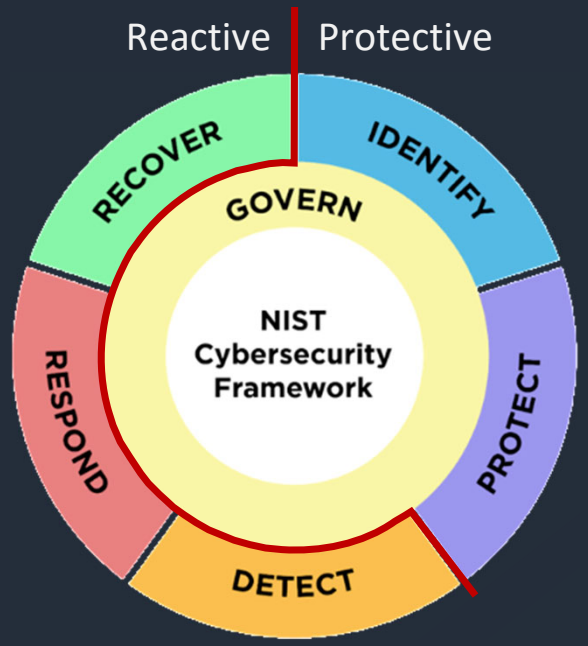
- Reporting obligations to CSIRT (in Denmark: CFCS)
  - Within 24 hours of discovery of incident: Early warning must be submitted
  - Within 72 hours of discovery of incident: Incident notification must be submitted
    - Severity and impact, Indicators of compromise
  - Within 1 month of handling incident: Final report
    - Detailed description of the incident, type of threat or root cause, applied and ongoing mitigation measures, cross-border impact of the incident

- Liability of management
  - Has to oversee and approve cybersecurity risk-management measures
  - Can be held liable for infringement
  - Needs to do awareness and training measures
    - Needs to offer it to employees as well

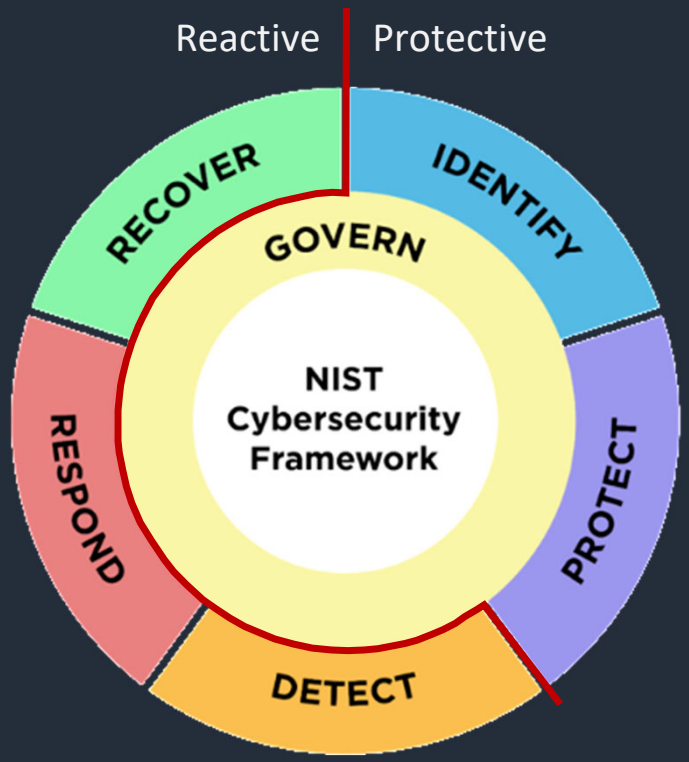
In 26% of companies management is not involved security decisions

NIST Cybersecurity Framework (CSF) 2.0

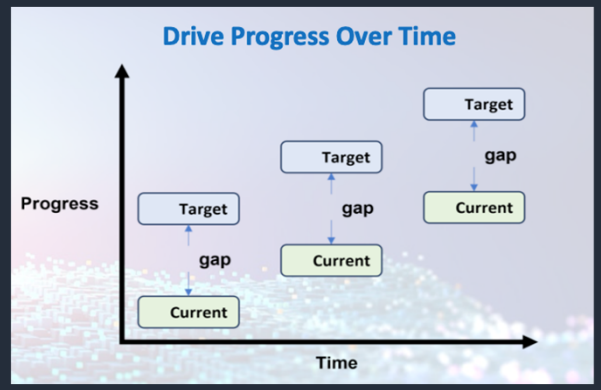
- NIST = US National Institute of Standards and Technology
- The CSF is guidance for sensible cybersecurity measures
- It is not a set of prescriptive guidance
  - Does not say how outcomes are achieved
- It is instead
  - Taxonomy for cybersecurity efforts and outcomes
  - Definition of functions and profiles



NIST CSF 2.0 Functions

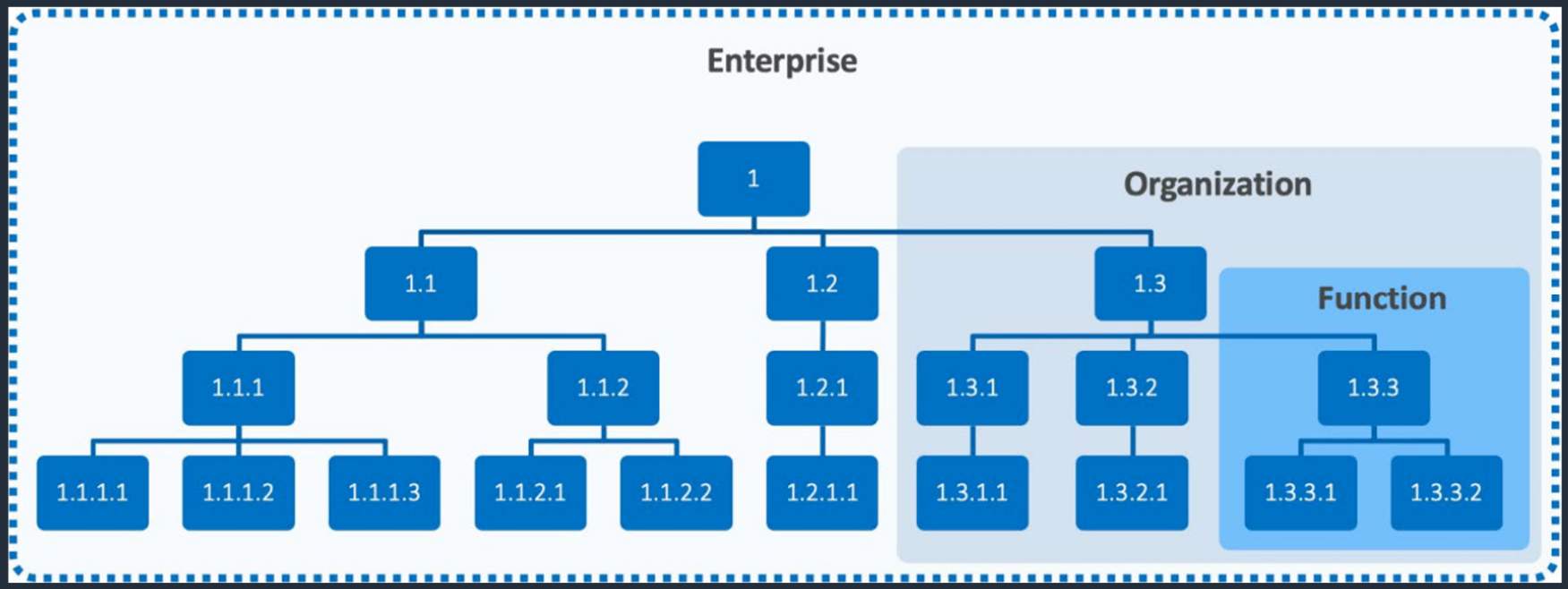


- Organisational Profiles
  - Further guidance to improve the cybersecurity posture of organisations
  - Current profile: describes outcomes that are currently achieved
  - Target profile: what the organisation is trying to achieve



Cybersecurity Capability Maturity Model (C2M2)

- Intended to strengthen organisations' cybersecurity capabilities



Cybersecurity Capability Maturity Model (C2M2)

- Maturity of cybersecurity capabilities is tracked for functions
  - Maturity Indicator Levels
  - Specifies process to improve capabilities

Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	Management characteristics: • Practices are documented • Adequate resources are provided to support the process Approach characteristic: • Practices are more complete or advanced than at MIL1
MIL3	Management characteristics: • Activities are guided by policies (or other organizational directives) • Responsibility, accountability, and authority for performing the practices are assigned • Personnel performing the practices have adequate skills and knowledge • The effectiveness of activities is evaluated and tracked Approach characteristic: • Practices are more complete or advanced than at MIL2

Response	Description
Fully Implemented	Complete
Largely Implemented	Complete, but with a recognized opportunity for improvement
Partially Implemented	Incomplete; there are multiple opportunities for improvement
Not Implemented	Absent; the practice is not performed by the organization

1. Reduce Cybersecurity Vulnerabilities	
MIL1	a. Information sources to support cybersecurity vulnerability discovery are identified, at least in an ad hoc manner b. Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner c. Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner d. Cybersecurity vulnerabilities that are relevant to the delivery of the function are mitigated, at least in an ad hoc manner
MIL2	e. Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored f. Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events

ISO 27001

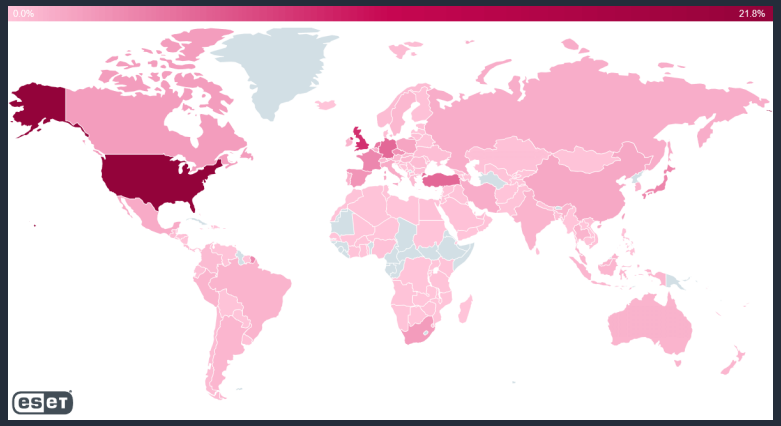
- International standard that allows certification of an organisation's information security management system (ISMS)
- Basically has same building blocks as other frameworks
  - Examine risks (threats, vulnerabilities, impacts)
  - Enact cybersecurity controls and risk management strategies
  - Adopt overarching management process

- Most important aspect: certification
  - Auditor inspects ISMS
  - Positive outcome results in compliance certification
  - Pitfall: Organisations might focus on compliance instead of actually achieving security capabilities

Supply Chain Cybersecurity Attacks in Practice

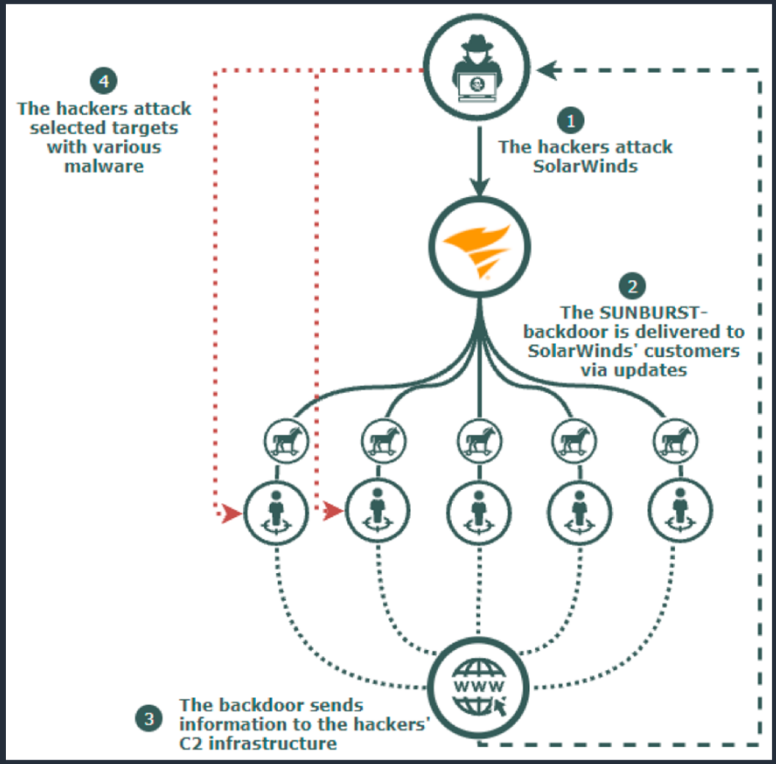
Case 1: Log4Shell Vulnerability

- Log4j Library: Logging functionality in Java software
- Log4Shell: Zero-day vulnerability allowing arbitrary remote code execution
- What has it to do with supply chains?
  - Used in many web applications
  - These applications can be contract work
  - Part of the digital supply chain for business operations
  - Unclear if the library has been used
  - Companies might be unaware of using it
  - As of 10.2024 still ~13% of applications online use vulnerable versions of the Log4j



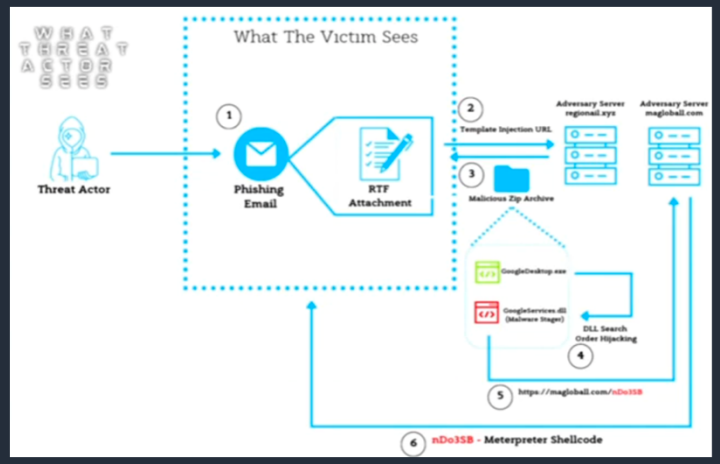
Case 2: SolarFlare Attack

- SolarWinds
  - Develops widely used IT network management system
  - Used by high-profile targets
- The attack
  - Hackers successfully got access to the SolarWinds internal network
  - The attackers compromised the software production platform and inserted a backdoor in the code
- A compromised update was released to 18000 customers 03-06.2020
  - US mostly affected, but also 150 victims in Denmark
  - Attributed to the Russian intelligence service SVR
- The other attack?
  - Evidence for parallel attack by a different threat actor



Case 3: South China Sea Hacks

- A range of attacks performed by Leviathan
  - Threat actor associated with Chinese Ministry of State Security
- Primary focus of operations
  - Espionage
  - Intellectual Property Theft
- Also involved in cyberattacks to disrupt supply chains in SCS
  - (Physical) Grey zone conflicts due to energy development projects
  - Leviathan used phishing attacks to target known suppliers



Questions?

https://sdu.dk/staff/mayer

@securitycapybara.bsky.social

Basics

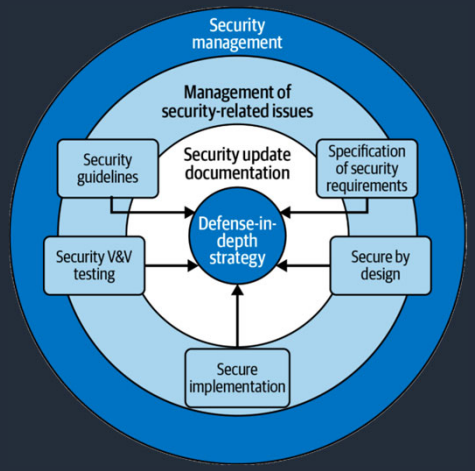
Best Practices

Frameworks & Standards

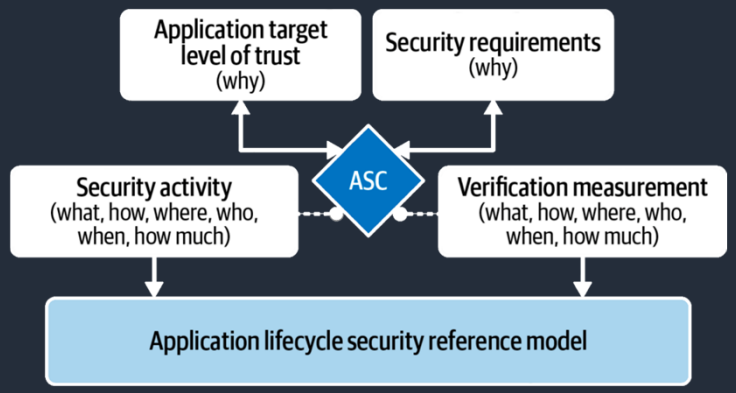
Attacks in Practice

Secure Software Development Standards

- **ISA/IEC 62443-4-1**
  Secure Development Lifecycle
  - Secure development process requirements for industrial automation and control systems products
  - Encompasses 8 practices



- **ISO/IEC 27034 Application Security**
  - Guidance for organizations acquiring, developing, or managing applications
  - Encompasses 5 main Elements



How much security is lost?

- Issue 1: People behave differently
  - Users required to change passwords frequently create less secure passwords and disclose them more often
  - Users annoyed with password policies choose weaker passwords

- Issue 2: Passwords are easy to guess based on previous one
  - *“we can break 17% of accounts on average in an online attack, with fewer than 5 online guesses in expectation”*
  - *“we can break future passwords from past ones using the same class of transforms in 63% of accounts on average in an offline attack”*

How much security is gained?

- ► Prevents continued access for attacker who relies on password
- ► Does not prevent continued access by backdoors, persistent malware, etc.

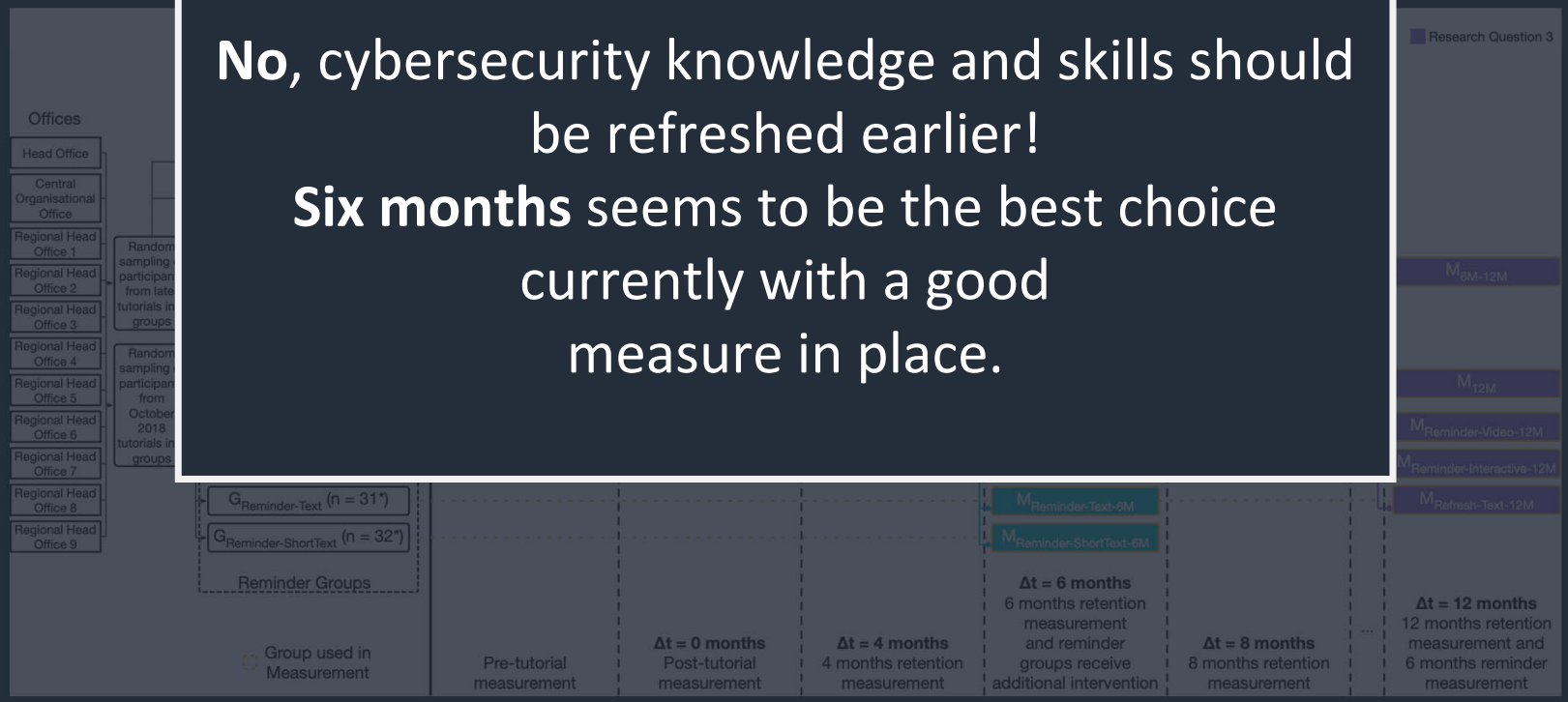
”the maximum advantage that a defender can hope to gain by a policy-driven password change is a reduction [in the expectation of attack success] from 1.0 […] to a probability […] in no cases any lower than 0.632”

“In sum, these security-specific observations and the results […] suggest the security benefit of password aging policies are at best partial and minor.”

Are 12 months a good time frame to refresh?

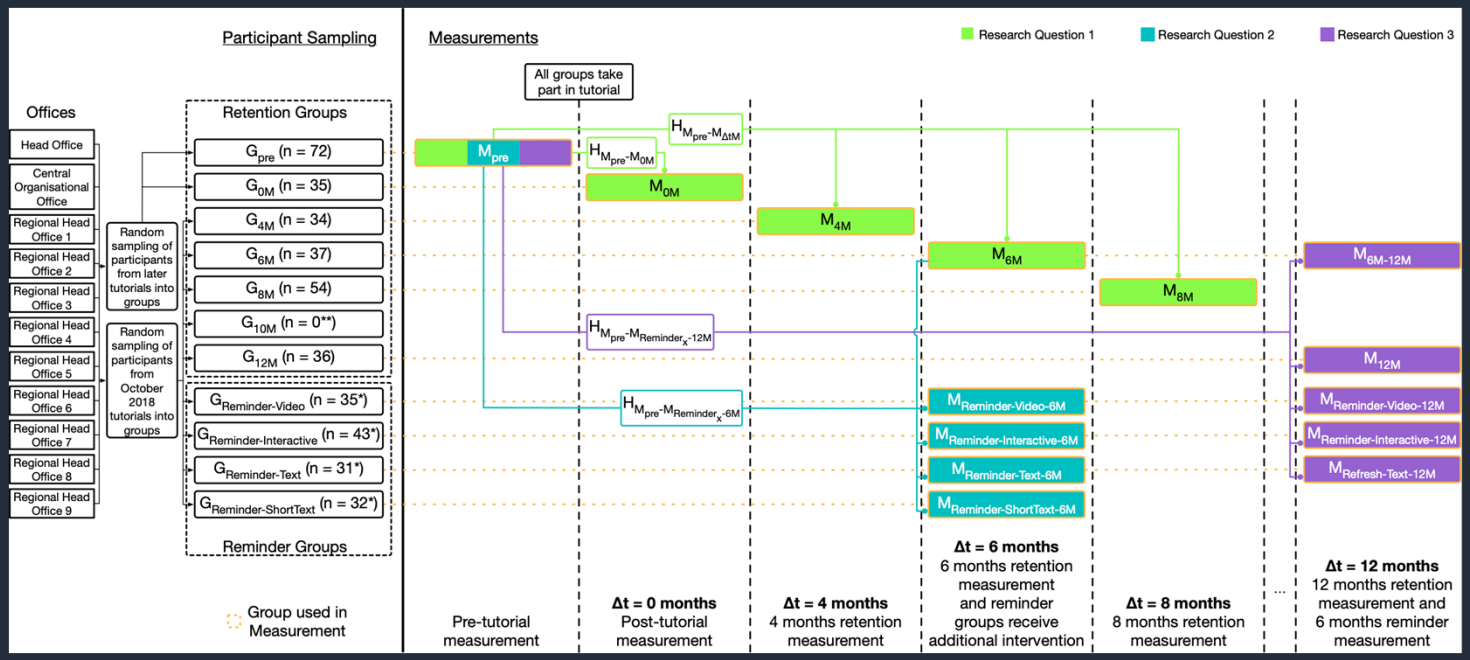
- Longitudinal evaluation over 12 months
  - Evaluation of effectiveness after 4, 6, 8 months
  - Reminder me

No, cybersecurity knowledge and skills should be refreshed earlier!
Six months seems to be the best choice currently with a good measure in place.



Are 12 months a good time frame to refresh?

- Longitudinal evaluation over 12 months
  - Evaluation of effectiveness after 4, 6, 8 months
  - Reminder measures introduced after 6 months, re-tested after 12



Can you use just any measure?

Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector

Mattia Mossano, *SECUSO, Karlsruhe Institute of Technology, Karlsruhe, Germany, mattia.mossano@kit.edu*
Kami Vaniea, *School of Informatics, University of Edinburgh, Edinburgh, United Kingdom, kvaniea@inf.ed.ac.uk*
Lukas Aldag, *SECUSO, Karlsruhe Institute of Technology, Karlsruhe, Germany, lukas.aldag@kit.edu*
Reyhan Düzgün, *SECUSO, Karlsruhe Institute of Technology, Karlsruhe, Germany*
Peter Mayer, *SECUSO, Karlsruhe Institute of Technology, Karlsruhe, Germany*
Melanie Volkamer, *SECUSO, Karlsruhe Institute of Technology, Karlsruhe, Germany*

We found that the overall quality of the analysed anti-phishing webpages is **in need of improvement**. […] Some of the anti-phishing webpages show **contradictory recommendations**, potentially heightening the frustration of the readers and leading to security fatigue. We argue that this **lack of consistent, up to date anti-phishing information** might be one of the causes why so many people are not able to detect phishing effectively.

Vision: What Johnny learns about Password Security from Videos posted on YouTube

Mathieu Christmann, Technical University of Darmstadt, Darmstadt, Germany, mathieu.christmann@gmail.com
Peter Mayer, peter.mayer@kit.edu, SECUSO - Security, Usability, Society, Karlsruhe Institute of Technology, Karlsruhe, Germany
Melanie Volkamer, melanie.volkamer@kit.edu, SECUSO - Security, Usability, Society, Karlsruhe Institute of Technology, Karlsruhe, Germany

ABSTRACT
The text password is the most pervasive authentication scheme and is unlikely to disappear soon. Companies employ password
medium sized companies (SMEs) are likely to refer their employees to available material on the Internet.
Our research aims to analyse the quality of freely available videos

In our analysis, we found that none of the existing videos fulfil all requirements. The best one covers only about half the requirements. Therefore, serious concerns regarding their suitability for awareness campaigns arise. It seems **none of them can be genuinely recommended to be used in such campaigns** – especially if the video is the only resource provided to the employees.

Evaluating Password Advice

Hazel Murray, Department of Mathematics and Statistics, Maynooth University, Ireland, Email: hazelmsmurray@gmail.com
David Malone, Hamilton Institute, Maynooth University, Ireland, E-mail: david.malone@nuim.ie

In this paper, we highlighted characteristics of the password advice currently available online. We show that there are **serious discrepancies in the advice given between sources**. We also note that some of the advice viewed by researchers and specialists as **"best practice" is often not represented by the majority of advice**. This contradictory information may reflect one of the reasons for users' unwillingness to follow advice.

Can you use just any measure?

Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector

Mattia Mossano
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany
mattia.mossano@kit.edu

Kami Vaniea
School of Informatics
University of Edinburgh
Edinburgh, United Kingd
kvaniea@inf.ed.ac.u

Lukas Aldag
SECUSO
Karlsruhe Institute of Technology

Reyhan Düzgün
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany

Peter Mayer
SECUSO
Karlsruhe Institute of Technology
Karlsruhe, Germany

We found that the overall quality of the analysed anti-phishing webpages is **in need of improvement**. [...] Some of the anti-phishing webpages show **contradictory recommendations**, potentially heightening the frustration of the readers and leading to security fatigue. We argue that this **lack of consistent, up to date anti-phishing information** might be one of
vely.

Vision: What Johnny learns about Pa
Videos posted on You

Mathieu Christmann
Technical University of Darmstadt
Darmstadt, Germany
mathieu.christmann@gmail.com

Peter Mayer
peter.mayer@kit.edu
SECUSO - Security, Usability, So
Karlsruhe Institute of Technolo
Karlsruhe, Germany

ABSTRACT
The text password is the most pervasive authentication scheme and is unlikely to disappear soon. Companies employ password

medium size
to available
Our resea

eos fulfil all requirements.
rious concerns regarding their
e genuinely recommended to
e provided to the employees.

No, effective measures are of the essence! So ask before getting one.

Evaluating Password Advice

Hazel Murray
Department of Mathematics and Statistics
Maynooth University, Ireland
Email: hazelmsmurray@gmail.com

David Malone
Hamilton Institute
Maynooth University, Ireland
E-mail: david.malone@nuim.ie

currently available online. We show that there are **serious discrepancies in the advice given between sources**. We also note that some of the advice viewed by researchers and specialists as **"best practice" is often not represented by the majority of advice**. This contradictory information may reflect one of the reasons for users' unwillingness to follow advice.

Examples of companies getting hacked

EU Network and Information Security (NIS) Directive

High Criticality Sectors

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health
- Drinking & waste water
- Digital Infrastructures
- ICT service management
- Public administration
- Space

Other Critical Sectors

- Postal & courier services
- Waste management
- Manufacture, production, and distribution of chemicals
- Production, processing, and distribution of food
- Manufacturing
- Digital providers (marketplaces, search engines, social networks)
- Research

Kind of “Critical Infrastructures*++”

*as defined in DIRECTIVE (EU) 2022/2557

Security Mindset

- Security experts need a specific mindset
  - Which parts do users have control over? Which ones shouldn’t they?
  - What can this do outside of what it is meant to do?
  - Is any of that unintended functionality useful?

This is annoying

I need to close this door

I should call maintenance

This sound will guide me to where I can get in

Security experts always look at the worst case