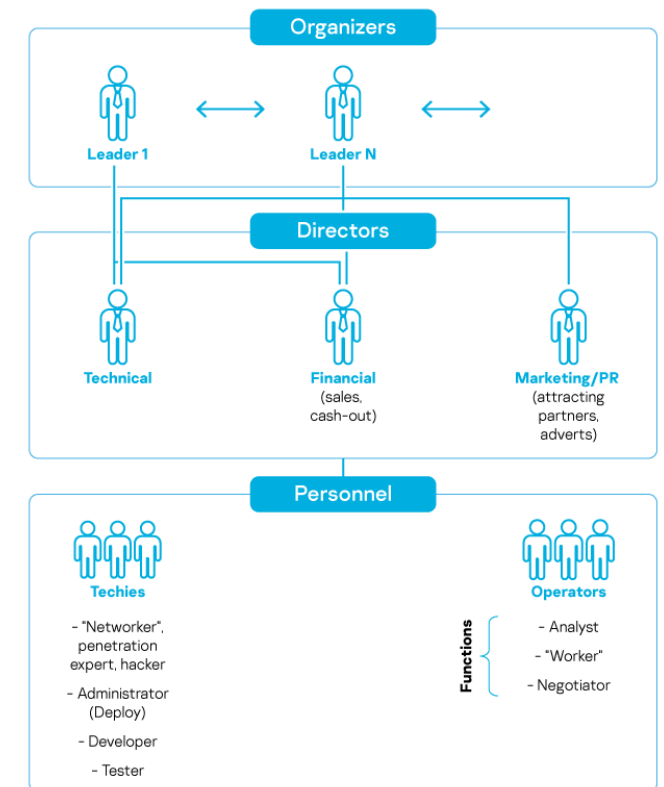


Security Landscape
and
Introduction to the course

David Crooks

Landscape: the world has changed

- In the past, biggest risk for academic security
 - Relatively simple, untargeted attacks
 - Belief that research computing was major risk
- This is no longer the case
 - Determined, well-resourced attackers
 - **9-5 jobs** working on malware services
 - Phishing and identity theft are major risk
 - Research computing security can be **major asset**
- Big business: we are targets



© 2021 AO Kaspersky Lab. All Rights Reserved

kaspersky

UK National Cybersecurity Centre

- [NCSC 2024 Report](#)

	Sep 2021 - Aug 2022	Sept 2022 - Aug 2023	Sep 2023 - Aug 2024
Total tips	1,226	2,005*	1,957
Incidents handled	355	371	430
Highly significant and significant incidents	62	62	89
Data exfiltration	276	327	347

- **Highly significant incident:** A cyber attack which has a serious impact on central government, UK essential services, a large proportion of the UK population, or the UK economy.
- **Significant incidents:** A cyber attack which has a serious impact on a large organisation or on wider/local government, or which poses a considerable risk to central government or UK essential services.
- *Increase in reports attributed to change in data collection and cannot be compared directly to previous years.

2024 ransomware

- Top sectors reporting ransomware
 - **academia**, manufacturing, IT, legal, charities and construction
- 317 reports of ransomware activity (up from 297)
- 20 NCSC managed incidents, of which 13 nationally significant
 - Includes British Library and NHS trusts

Incidents in or near our sector

[British Library](#)

LEARNING LESSONS FROM THE CYBER-ATTACK

British Library cyber incident review

8 MARCH 2024

[Home](#) | [Newsroom](#)

BESSY II back in operation after cyber attack on Helmholtz-Zentrum Berlin (HZB)

Incidents in or near our sector

ALMA

ALMA Has Successfully Restarted Observations



Credit: Carlos Padilla

Forty-eight days after suspending observations due to a cyberattack, the Atacama Large Millimeter/submillimeter Array (ALMA) is observing the sky again. The computing staff has worked diligently to rebuild the affected JAO computer system servers and services. This is a crucial milestone in the recovery process.

On 29 October, ALMA suffered a cyberattack. The computing staff took immediate countermeasures to avoid loss and damage to scientific data and IT infrastructure. The attack affected various critical operational servers and computers.

Lincoln College, IL

Lincoln College to close after 157 years due ransomware attack

By [Sergiu Gatlan](#)

May 9, 2022 06:17 PM 4



Lincoln College, a liberal-arts school from rural Illinois, says it will close its doors later this month, 157 years since its founding and following a brutal hit on its finances from the COVID-19 pandemic and a recent ransomware attack.

BL lessons learned

- Enhance network monitoring capabilities
- Retain on-call external security expertise
- Fully implement multi-factor authentication
- Enhance intrusion response processes
- Implement network segmentation
- Practice comprehensive business continuity plans
- Maintain a holistic overview of cyber-risk
- Manage systems lifecycles to eliminate legacy technology
- Prioritise remediation of issues arising from legacy technology
- Prioritise recovery alongside security
- Cyber-risk awareness and expertise at senior level
- Regularly train all staff in evolving risks
- Proactively manage staff and user wellbeing
- Review acceptable personal use of IT
- Collaborate with sector peers
- Implement Government standards, review and audit policies and processes regularly

Approach

- Over last years we have seen very high-profile attacks
 - Particularly ransomware
 - Many in the press
- For an organisation an attack can be **catastrophic**
 - Months of complete organisational shutdown
- It is **essential** that we work together to defend our community

Motivation for this school

- Talked yesterday about the motivation for this school
- Emphasise training and skills for system managers and others deploying IT capabilities
 - Alongside cybersecurity professional colleagues
- Build community of practice around security in our sector

Security frameworks and research computing

- Broad historical experience of the relationship between research computing security and corporate IT security
 - Often challenging
 - Necessarily more open risk appetite required for research computing may be at odds with corporate IT risk appetite
 - Research computing may well require **different** controls, but it still requires controls
- Frameworks help in a research context as much as anywhere else

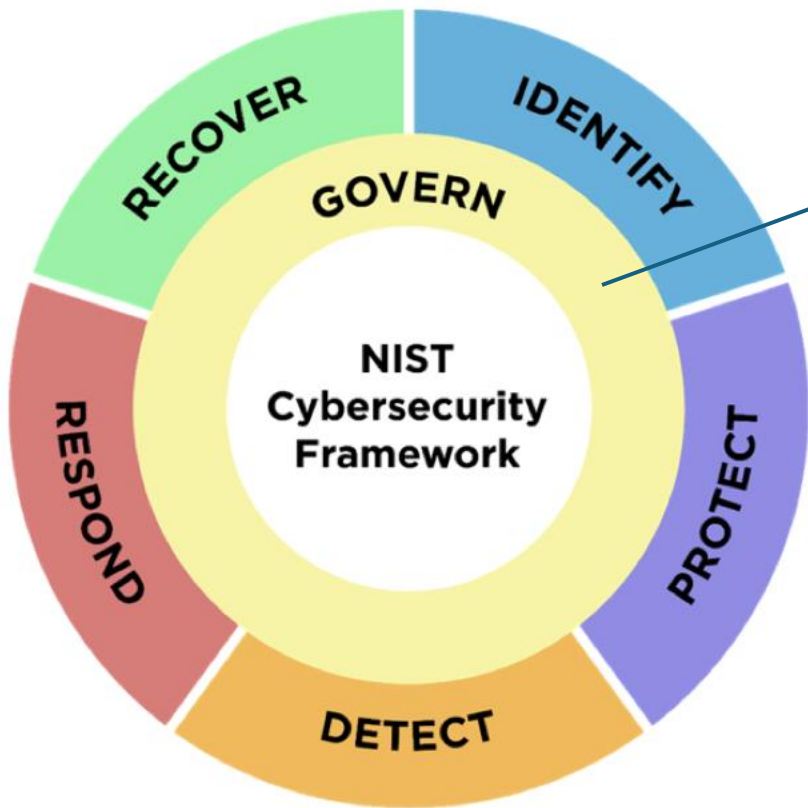
About the program: frameworks

- Not getting into the meat of the course yet, but...
- Note the importance of security frameworks in supporting and driving this work
 - Compliance can be useful!
- ISO27k, UK NCSC Cyber Assessment Framework, NIST Cybersecurity Framework

About the program: frameworks

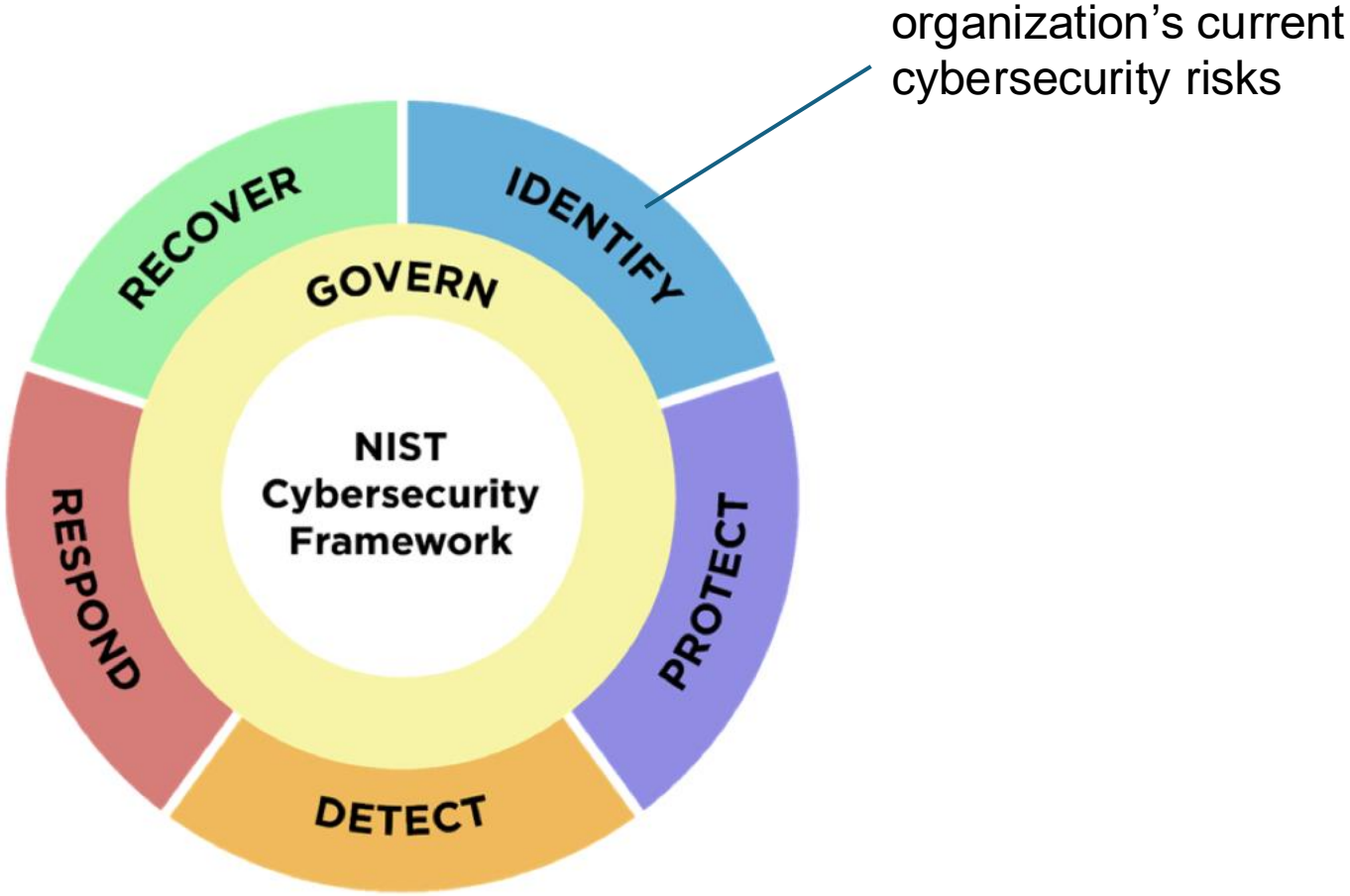


About the program: frameworks

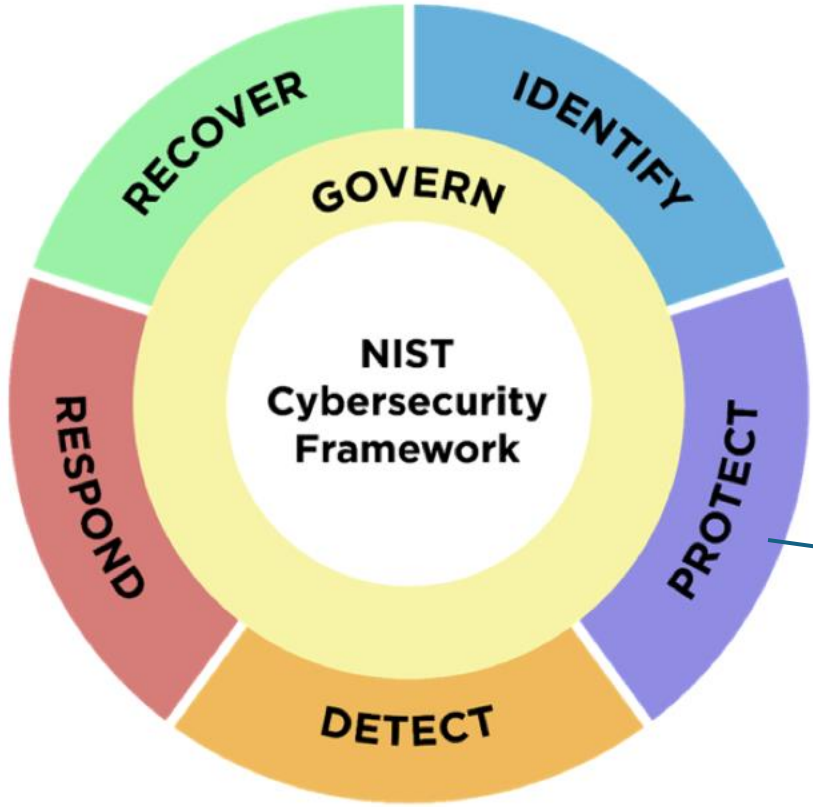


organization's cybersecurity risk management strategy

About the program: frameworks



About the program: frameworks



safeguards to manage the organization's cybersecurity risks

About the program: frameworks



possible cybersecurity attacks and compromises are found and analyzed

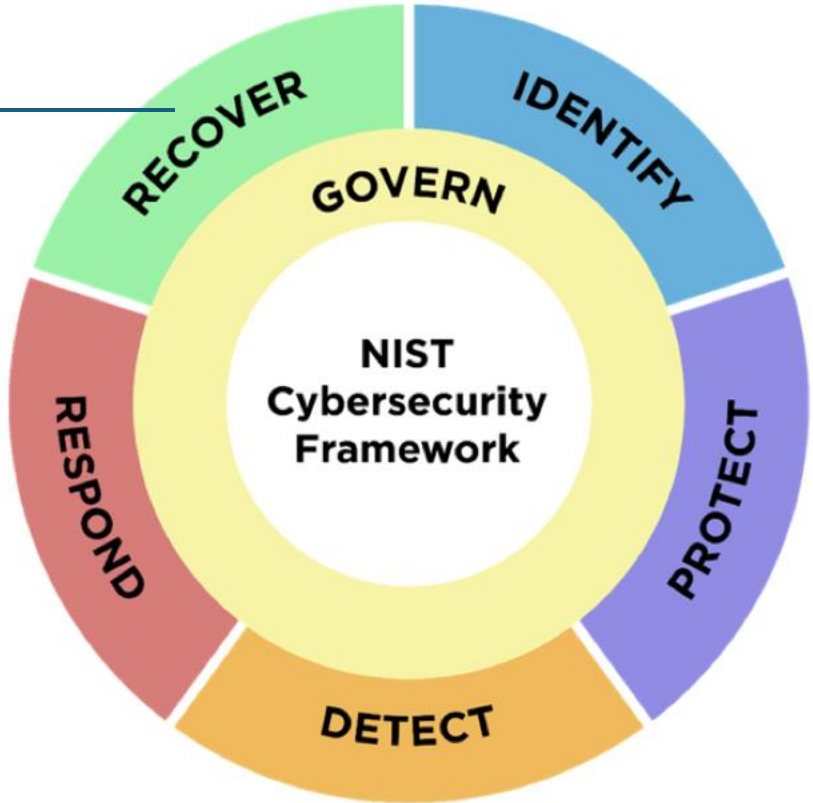
About the program: frameworks



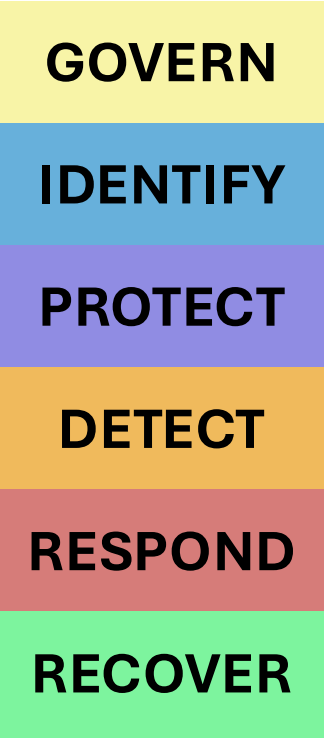
actions regarding a detected cybersecurity incident are taken

About the program: frameworks

assets and operations affected by a cybersecurity incident are restored



About the program: frameworks



← You are here!



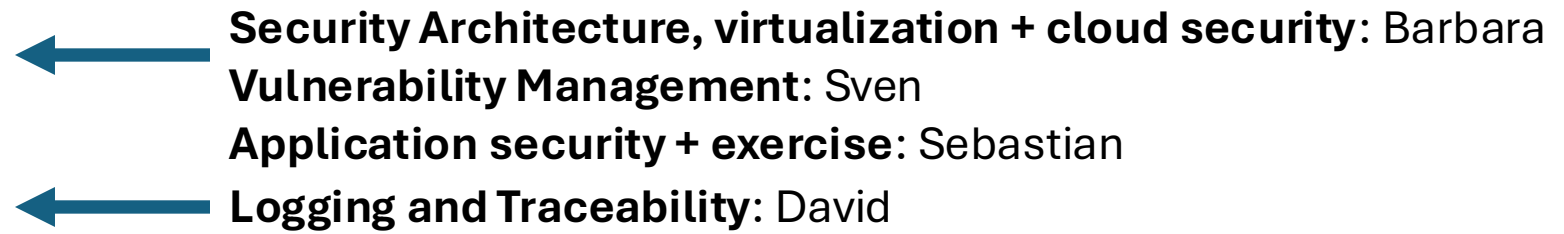
Monday



← Risk Management: Sven

← Security Architecture: Barbara
Identity, Authentication and Authorisation + exercise: Tom

Tuesday



Wednesday

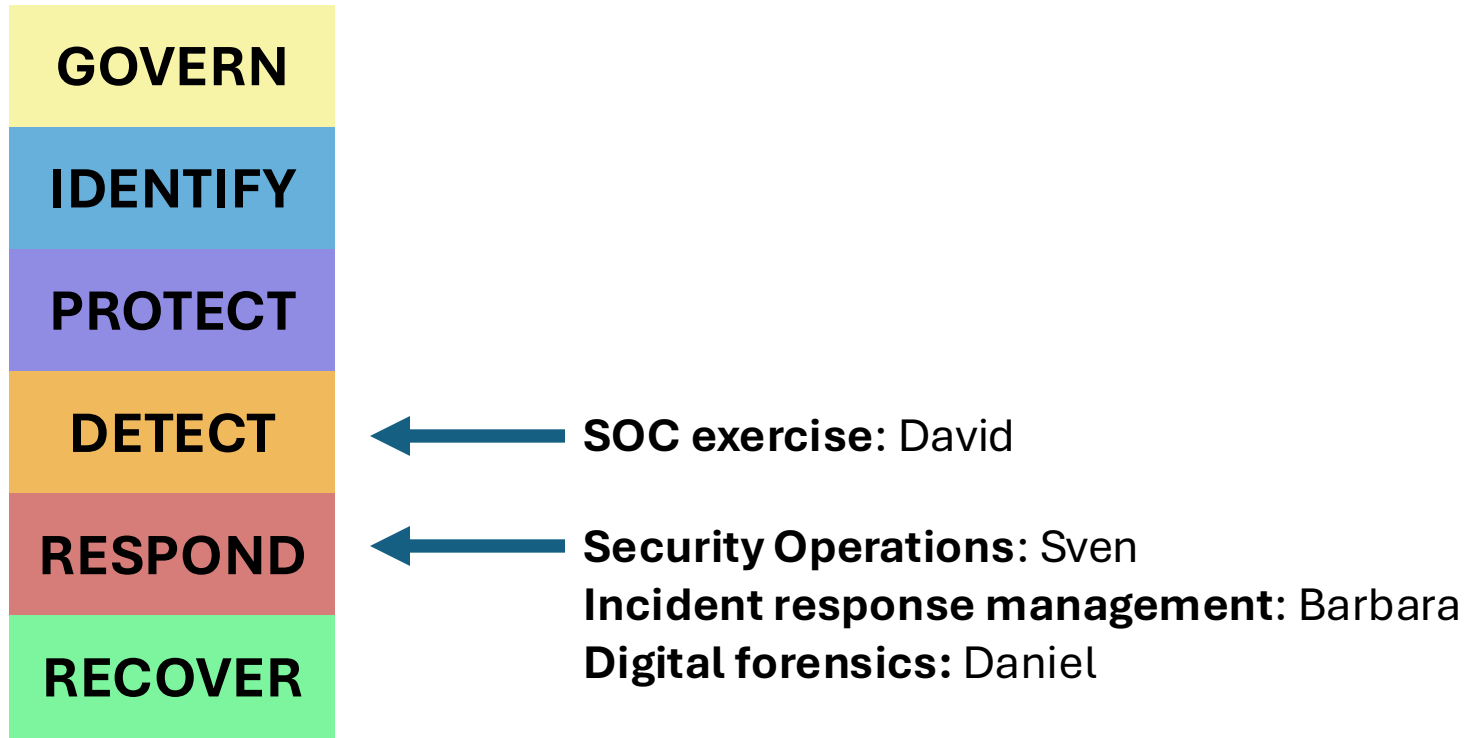


Container security: Daniel



Security Operations Centres: David

Thursday



Friday



← **Pentesting debrief:** Sebastian

← **Digital forensics exercises:** Daniel
Incident response exercise: Tutors

On to the lectures

- First lecture:
- 1130: Risk management with Sven