BUSINESS ANALYSIS CONFERENCE EUROPE

16 - 18 September 2024 • London, UK

Please score and comment on this session and speaker in the event mobile app

IRMUK

A Masterclass In
Security And Quality Requirements Engineering

A Masterclass In Security And Quality Requirements Engineering

Presented by
Mark Cross from Envista Consulting
18th August 2024

ABOUT THE SPEAKER

MARK CROSS
PRINCIPAL CONSULTANT
ENVISTA CONSULTING

Mark Cross has been working in IT transformation for twenty-five years. He spent ten years as a network engineer in leading telcos before switching to a career in business analysis. As a business analyst, his areas of specialism include cloud transformation, data migration, information protection and cybersecurity. He has a passion for helping organisations to reduce their security debt and their exposure to cyber-risk.

He holds an MBA from Alliance Manchester Business School, the International Diploma in Business Analysis and Chartered IT Professional status from the British Computer Society. He also holds the Certified Business Analysis Professional (CBAP) and Certified Cybersecurity Analyst (CCA) credentials from the International Institute of Business Analysis and the Certified Information Systems Security Professional (CISSP) credential from ISC2.

He is the founder and principal consultant of Envista Consulting, the regional lead for Yorkshire Cybersecurity Cluster in North Yorkshire and serves on the committee of the IIBA UK North Branch.

A CYBERSECURITY JOURNEY IN FOUR PARTS

Business Analysis Circa 2000
Focused on Utility, Interoperability and Quality

Business Analysis Circa 2010
Focused on Agility, Efficiency and Speed to Market

Business Analysis Circa 2020
Focused on Scalability, Mobility and User Experience

Business Analysis Circa 2030
Focused on Security, Resilience and Intelligence.

Find out more at https://envistaconsulting.com

AGENDA FOR TODAY

9:30 AM: First Part Begins

- Current Threats
- What Is Quality in Security?
- The Delivery Lifecycle
- What can go wrong, and what we can do about it?

11:00 AM: Morning Break

11:30 AM: Second Part Begins

- The SQUARE Method
- Common Definitions
- Cyber-Risk Assessments
- Prioritisation 2.0

13:00 PM: Lunch

Part 1

THE GROWING NEED FOR SECURITY

CYBER-ATTACKS ARE EVERYWHERE

The Standard

NEWS I UK

How to know if your details were leaked in TfL hack: Everything we know so far

Transport for London doesn't know when it will recover from 'very sophisticated' cyber attack, admits tech chief

TFL SAID SOME CUSTOMER DATA WAS ACCESSED IN THE CYBER ATTACK (KATIE COLLINS/PA)

PA ARCHIVE

FINANCIAL TIMES

British Library to burn through reserves to recover from cyber attack

London-based institution faces spending millions of pounds to rebuild most digital services

Rafe Uddin and Daniel Thomas in London JANUARY 5 2024 286

The British Library will drain about 40 per cent of its reserves to recover from a cyber attack that has crippled one of the UK's critical research bodies and rendered most of its services inaccessible.

The London-based institution, which stores nearly 170mn pieces of work ranging from books to sound recordings, was forced offline in October after a "deep and extensive" ransomware attack.

Hackers published hundreds of thousands of stolen files online, including customer and personnel data, after the library refused to pay a £600,000 ransom. But it will now be forced to spend about 10 times that amount rebuilding most digital services at an estimated cost of £6mn-£7mn, according to a person familiar with the matter, consuming a sizeable proportion of its £16.4mn in unallocated reserves.

The British Library's online catalogue remains unavailable. Physical sites are open, but users must wait while librarians run through logs and find items on shelves.

Support the Guardian

Fund independent journalism with £10 per month

The Guardian

News Opinion Sport Culture Lifestyle More

NHS

Cyber-attack on London hospitals to take 'many months' to resolve

Exclusive: NHS source says clarity needed on how Russian hackers gained access and whether records are retrievable

Denis Campbell and Dan Milmo

Tue 11 Jun 2024 12.27 BST

Share

Six NHS trusts and scores of GP practices in south-east London have been struggling to deliver many types of care since the attack. Photograph: Alicia Canter/The Guardian

The cyber-attack that is causing serious disruption for hospitals and GP surgeries in London will take "many months" to resolve, a senior NHS source has warned.

"It is unclear how long it will take for the services to get back to normal, but it is likely to take many months," the well placed official said.

"Key to a return to normal will be clarity about how the hackers gained access to the system, how many records have been affected and whether these records are retrievable," they added.

Six NHS trusts and scores of GP practices in south-east London, which serve 2 million patients, have been struggling to deliver many types of care normally to patients since Russian hackers infiltrated and rendered unusable the IT system of Synnovis, a private firm which analyses blood tests.

SECURITYWEEK NETWORK: Cybersecurity News Webcasts Virtual Events ICS Cybersecurity Conference

SECURITYWEEK CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

CYBER INSURANCE

MGM Resorts Says Ransomware Hack Cost $110 Million

MGM Resorts said costs from a disruptive ransomware hack has exceeded $110 million, including $10 million in one-time consulting cleanup fees.

By Ryan Naraine
October 6, 2023

Hospitality and entertainment giant MGM Resorts said costs from last month's debilitating ransomware infection have exceeded $110 million, including $10 million in one-time consulting clean-up fees.

In an SEC 8-K filing, MGM Resorts said the data-extortion attack caused operational disruptions, especially in its Las Vegas properties, and an estimated financial toll that includes about $100 million in lost revenue.

MGM Resorts, which manages prominent hotels like Mandalay Bay (site of the Black Hat security conference), Bellagio, MGM Grand, Aria, Luxor and the Cosmopolitan, said it also shelled out $10 million for technology consulting services, legal fees and expenses of other third party advisors.

The company confirmed "disruptions" at some of its properties but said the breach did not cause the loss of any customer bank account numbers or payment card details.

ars TECHNICA

HIGH-PRESSURE TACTIC —

Ransomware group reports victim it breached to SEC regulators

Group tells SEC that the victim is in violation for not reporting it was hacked.

DAN GOODIN - 11/17/2023, 12:03 AM

90

One of the world's most active ransomware groups has taken an unusual—if not unprecedented—tactic to pressure one of its victims to pay up: reporting the victim to the US Securities and Exchange Commission.

The pressure tactic came to light in a post published on Wednesday on the dark web site run by AlphV, a ransomware crime syndicate that's been in operation for two years. After first claiming to have breached the network of the publicly traded digital lending company MeridianLink, AlphV officials posted a screenshot of a complaint it said it filed with the SEC through the agency's website. Under a recently adopted rule that goes into effect next month, publicly traded companies must file an SEC disclosure within four days of learning of a security incident that had a "material" impact on their business.

The Verge

TECH Updated Dec 21, 2023, 7:07 PM GMT

Lapsus$ cyberattacks: the latest news on the hacking group

By Emma Roth, a news writer who covers the streaming wars, consumer tech, crypto, social media, and much more. Previously, she was a writer and editor at MUO.

The Lapsus$ hacking group first made headlines when it waged a ransomware attack against the Brazilian Ministry of Health in December 2021, compromising the COVID-19 vaccination data of millions within the country.

Since then, it has targeted a number of high-profile technology companies, stealing data from Nvidia, Samsung, Microsoft, and Vodafone. Lapsus$ also managed to disrupt some of Ubisoft's services and also gained access to an Okta contractor's laptop, putting the data of thousands of companies that use the service at risk. It's also suspected to be behind last year's attack on EA Games.

Shortly after the attack on Okta, a report pinned an England-based teenager as the mastermind behind the hacking group and said another teen member may reside in Brazil. One member of the group is reportedly so skilled at hacking that researchers thought their work was automated. On March 24th, the London police made seven arrests in connection with the Lapsus$ group, all of whom are teenagers.

BLEEPINGCOMPUTER

Home › News › Security › UnitedHealth subsidiary Optum hack linked to BlackCat ransomware

UnitedHealth subsidiary Optum hack linked to BlackCat ransomware

By Sergiu Gatlan February 28, 2024 07:13 PM 1

A cyberattack on UnitedHealth Group subsidiary Optum that led to an ongoing outage impacting the Change Healthcare payment exchange platform was linked to the BlackCat ransomware group by sources familiar with the investigation.

Change Healthcare warned customers on Wednesday that some of its services are offline because of a cybersecurity incident. One day later, UnitedHealth Group said in an SEC 8-K filing that the cyberattack was coordinated by suspected "nation-state" hackers who gained access to Change Healthcare's IT systems.

THE HYPER CONNECTED CLOUD














WHY IS EVERYTHING “CYBER” NOW?

Is this just another buzzword?

EVOLUTION OF BUSINESS INFORMATION SYSTEMS

THE PRE-DIGITAL ERA

TRADITIONAL INVENTORY

TRADITIONAL INFORMATION STORAGE

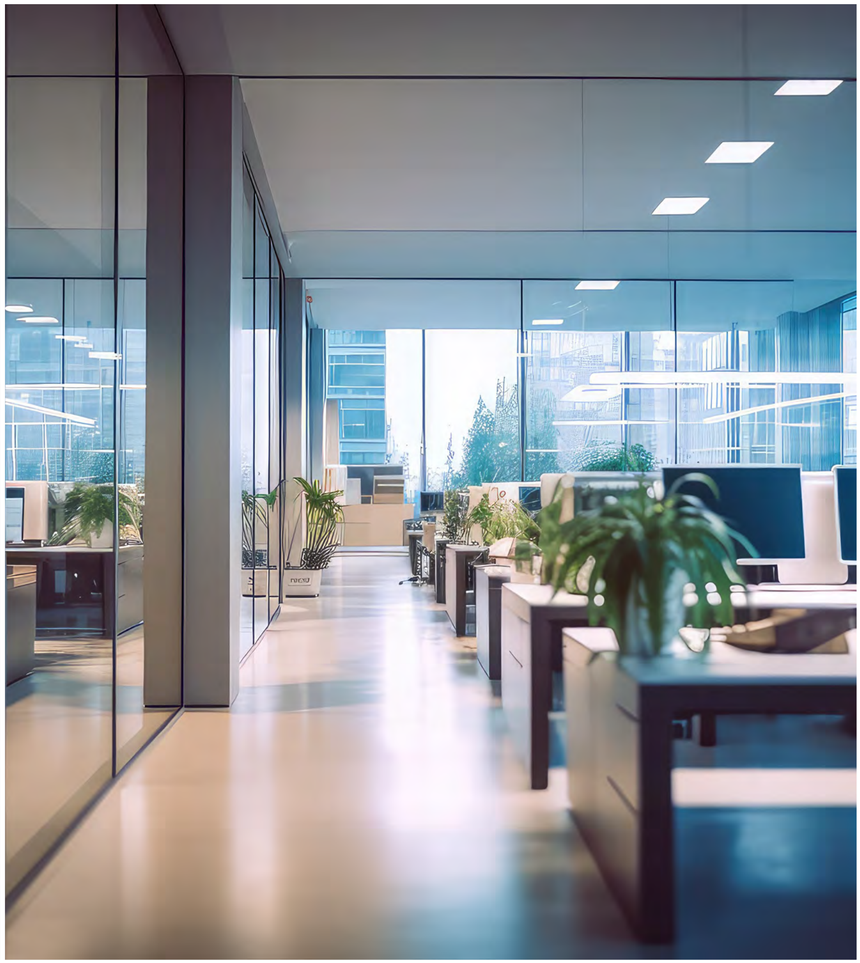
TRADITIONAL BUSINESS

EVOLUTION OF BUSINESS INFORMATION SYSTEMS

THE DIGITAL ERA

RECENT INVENTORY

RECENT INFORMATION STORAGE



RECENT BUSINESS

EVOLUTION OF BUSINESS INFORMATION SYSTEMS

THE CYBER ERA

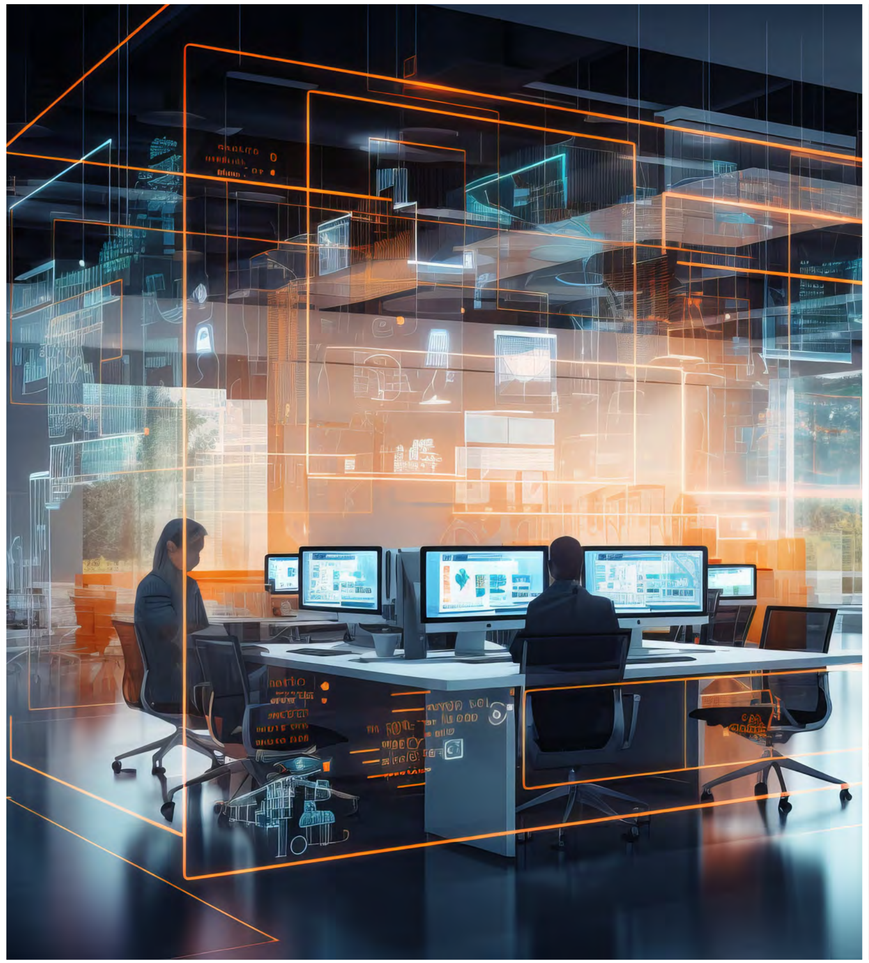
MODERN INVENTORY

MODERN INFORMATION STORAGE

MODERN BUSINESS

THE IMPORTANCE OF CYBER-RESILIENCE

Cash, Clouds and a $125 Billion Dollar Catastrophe



Sources:

https://www.unisuper.com.au/about-us/media-centre/2024/a-joint-statement-from-unisuper-and-google-cloud

https://cloud.google.com/blog/products/infrastructure/details-of-google-cloud-gcve-incident

SOLARWINDS

How Bad Can Twelve Lines Of Code Possibly Be?

Sources:

https://www.solarwinds.com/sa-overview/securityadvisory/faq

https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/solarwinds

MEET YOUR OPPONENTS…

Motivated By An Ideology

Motivated By Financial Reward

LIFTING THE VEIL ON CYBERCRIME

THE BUSINESS MODEL OF A CYBERCRIMINAL

It's simple math!

Cost to develop ransomware
- 160 hours at $200/hour

Cost of disposable infrastructure
- 10 servers at $500 ($50/server)

Cost of launching ransomware attack
- Push "button" to start
- Monitor for 10 days (240 hours at $150/hour)

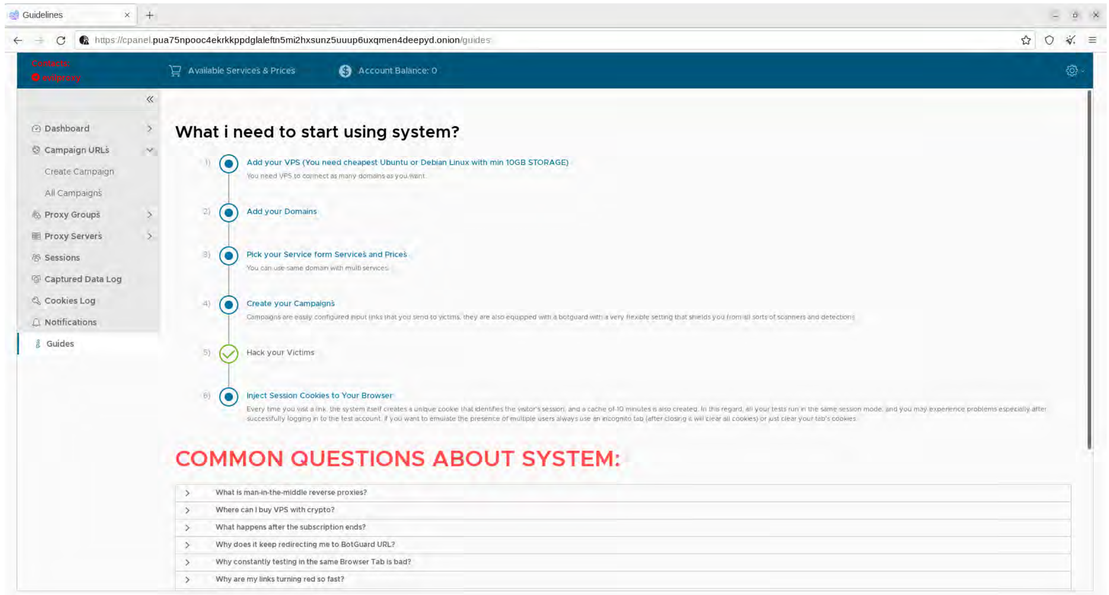
Attack 1,000,000 targets
- 1% pay the ransom at $300/system

	Cost
Developer	$32,000
Infrastructure	$500
Launch attack	$50
Help desk	$36,000
Investments	$68,550
1% target market share	$3,000,000
Return on investment	**$2,931,450**

The Business Case For Ransomware

Source:

https://www.isaca.org/resources/white-papers/blueprint-for-ransomware-defense



EvilProxy – Phishing As A Service

Source:

https://www.infosecurity-magazine.com/news/evilproxy-phishing-attack-strikes/

Further Reading on Ransomware as a Service:

https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

THE UK RESPONSE TO THIS THREAT...

In July 2024, the incoming UK government announced a new Cyber Security and Resilience Bill

The Bill updates the existing regulatory framework by expanding the regulations to protect more digital services and supply chains. This may also include new powers to proactively investigate potential vulnerabilities, mandatory incident reporting and cost recovery mechanisms (fines).

These steps are intended to give the government better data on cyber attacks, including where a company has been held to ransom - improving our understanding of the threats and alert us to potential attacks.

Sources:

https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pdf

https://www.ncsc.gov.uk/blog-post/legislation-help-counter-cyber-threat-cni

Part 2

UNDERSTANDING SECURITY + RESILIENCE

SECURITY + RESILIENCE

AND HOW ARE THEY CONNECTED?

SECURITY:

Protecting against bad people doing bad things.

RESILIENCE:

Protecting against bad processes and bad luck.

THE #1 MISTAKE WITH ENTERPRISE SECURITY

THE PROBLEM WITH A SINGLE LINE OF DEFENCE

WHAT YOU SEE:

...

WHAT YOUR ATTACKER SEES:

...

WHAT IS DEFENCE IN DEPTH?

BUILDING A MORE SECURE ENTERPRISE

BUILD MULTIPLE LAYERS OF DEFENCE

...

...OF MANY DIFFERENT KINDS

...

THE BASICS OF THE CIA TRIAD

The simplest and most fundamental properties of security are defined by a model called the “CIA Triad”.

The letters “CIA” stand for:

- Confidentiality
- Integrity
- Availability

When people think of information security, the most common one that they think about is confidentiality. Although a loss of any of these qualities would devalue of an information asset and may expose the organisation to undesirable consequences.

What Is CONFIDENTIALITY?

Confidentiality is the quality of knowing that your data cannot be and has not been read by anyone other than authorised users for legitimate reasons.

Examples of failures of confidentiality include:

- Documentation being placed in a file share an exposed to people who do not have authorisation to view it, or
- Changing permissions of a file share that already contains sensitive information in a way that allows unauthorised people to view it.
- A member of staff looking up the records of a specific individual without having a business justification to do so.
- Someone looking at sensitive information on an exposed computer screen or printed document.
- Disposing of sensitive information without it being destroyed securely.

What Is INTEGRITY?

Integrity is the quality of your data remaining intact and unmodified after creation unless it is intentionally changed.

Failures of integrity can include issues such as:

- Data on magnetic storage devices can become corrupted due to exposure to electromagnetic interference.
- Optical storage media can be affected by scratches or residue on the media.
- Corruption due to system failures or synchronisation errors.

What is AVAILABILITY

Availability is the quality of knowing that your data and services will be accessible and functional when you need them to be.

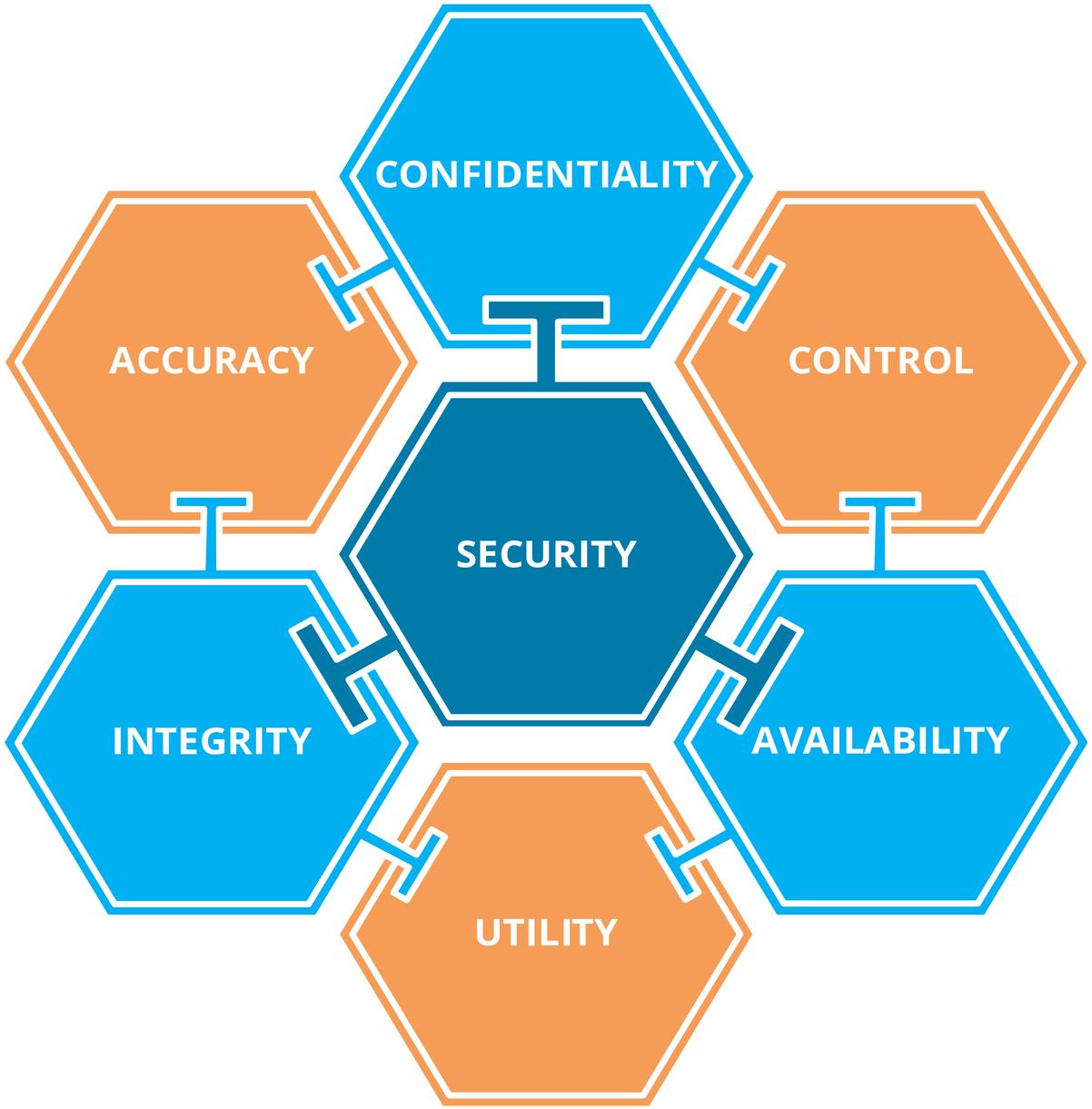
Common causes of loss of availability include:

- Lack of sufficient network or system processing capacity to respond to queries.
- Changes to network configuration that may prevent data from being exchanged between a client and the server.
- Systems being powered down, damaged or under maintenance.

THE SIX QUALITIES OF GOOD SECURITY

(The Parkerian Hexad)

The Triad has been extended for the digital age...



Find out more at https://envistaconsulting.com

EXPLORING THE PARKERIAN HEXAD

Three New Qualities Of Security For The Digital World

ACCURACY

Accuracy is the quality of information being correct, or at least ensuring that it comes from a legitimate source. This also includes the capability to provide irrefutable evidence of key events such as the exchange of legal contracts or an audit trail surrounding critical decisions.

UTILITY

Utility is the quality of an information system demonstrating the behaviour that is expected of it. The most well-known example of a failure of utility is the classic (encryption-only) ransomware attack. All systems are contactable and recoverable, however they are unable to be used for their intended purpose.

CONTROL

Control (also known as possession) is the quality of having the ability to exclusively manage access to or the behaviour of an information system without being subject to another party.

Note: Theft of the system itself is also considered to be a loss of control.

Part 3

THE DELIVERY LIFECYCLE

CREATING CHANGES IN YOUR ORGANISATION

A SIMPLIFIED DELIVERY LIFECYCLE

ANALYSIS AND PLANNING

DESIGN AND BUILD

TESTING AND RELEASE

IN SERVICE

CREATING CHANGES IN YOUR ORGANISATION

THE POINT AT WHICH YOU START THINKING ABOUT SECURITY MATTERS

ANALYSIS AND PLANNING

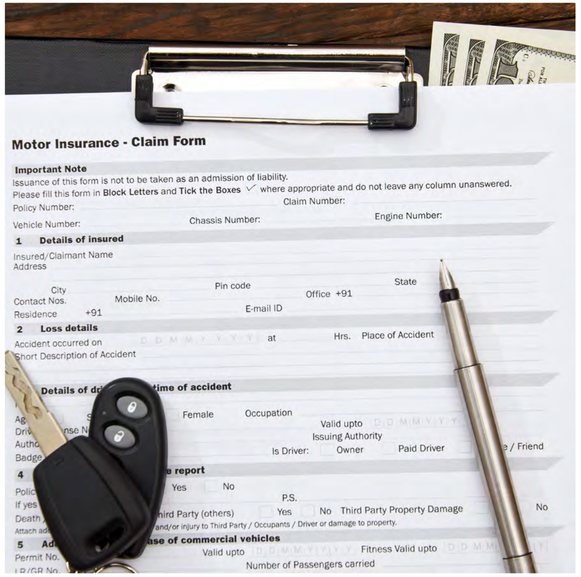
Projects that adopt a “Secure-by-Design” philosophy deliver products that are both secure and functional at little or no extra cost. This is the ideal scenario.

DESIGN AND BUILD

There is still early enough to deliver a secure, working product however it may require adding additional features to secure what has already been built. This can lead to cost overruns and delays.

TESTING AND RELEASE

It is now too late to make major changes to the product without impacting the delivery dates and budget. Fixing any new security issues will likely require a trade-off between limiting unsafe functionality or accepting the risk.



IN SERVICE

Once in service, the risk is immediate and costly to remediate. Security incidents evolve rapidly and if not contained within the first few minutes, they can lead to significant losses.

CREATING CHANGES IN YOUR ORGANISATION

THE POINT AT WHICH YOU START THINKING ABOUT SECURITY MATTERS

ANALYSIS AND PLANNING

Risk can be **CONTROLLED**

PREVENTATIVE measures are possible.

(ie: secure-by-design application development)

DESIGN AND BUILD

Risk can be **MANAGED**

ADAPTIVE measures are possible.

(ie: Deploying new firewall rules, access controls and malware filtering)

TESTING AND RELEASE

Risk can be **MEASURED**

Some **RESPONSIVE** measures are possible.

Such as: Incident response planning and Monitoring tools

IN SERVICE

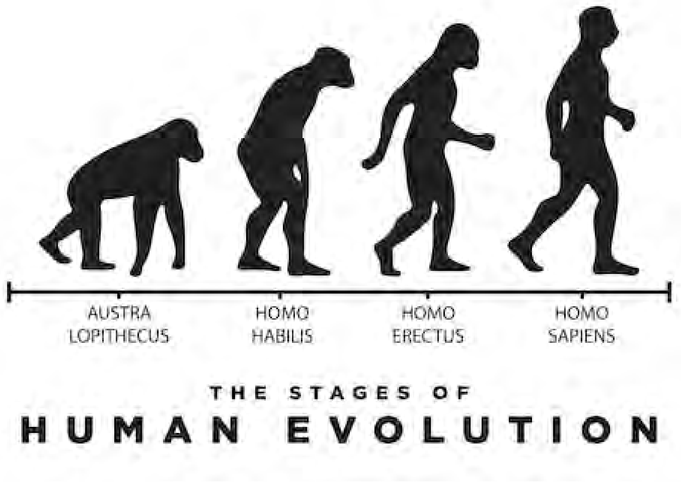
Risk is **UNCONTROLLED**

Only **REACTIVE** measures are possible

THREE APPROACHES TO SECURITY REQUIREMENTS

The Good, The Bad and the Ugly

THE “DO-NOTHING” APPROACH



THE “MATURITY MODEL” APPROACH

THE “RISK BASED” APPROACH

CREATING CHANGES IN YOUR ORGANISATION

THE POINT AT WHICH YOU START THINKING ABOUT SECURITY MATTERS

ANALYSIS AND PLANNING

Risk can be **CONTROLLED**

PREVENTATIVE measures are possible.

(ie: secure-by-design application development)

DESIGN AND BUILD

Risk can be **MANAGED**

ADAPTIVE measures are possible.

(ie: Deploying new firewall rules, access controls and malware filtering)

TESTING AND RELEASE

Risk can be **MEASURED**

Some **RESPONSIVE** measures are possible.

Such as: Incident response planning and Monitoring tools

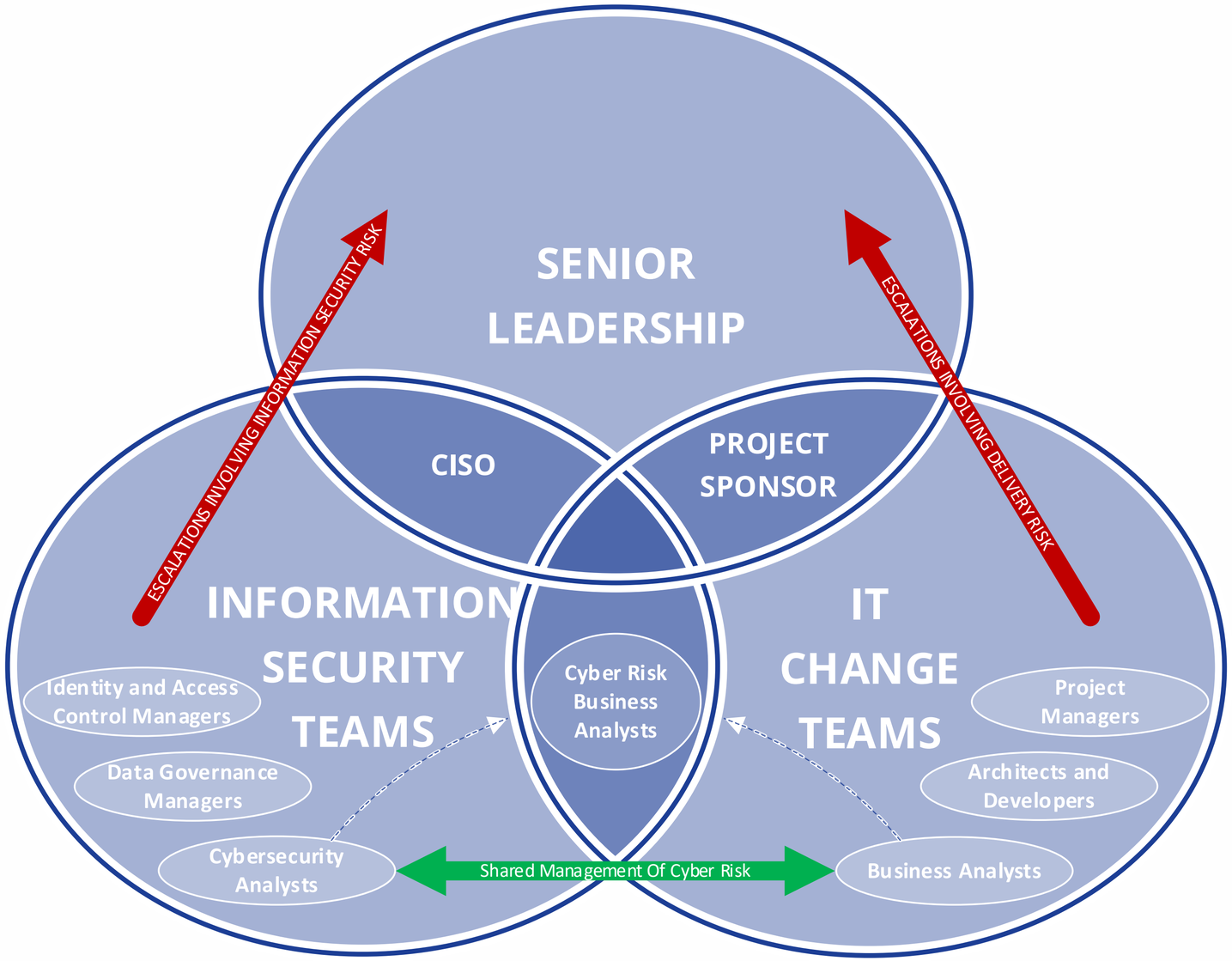
IN SERVICE

Risk is **UNCONTROLLED**

Only **REACTIVE** measures are possible

THE DIFFERENCE THAT A BUSINESS ANALYST CAN MAKE

...



THE ART OF MANAGING AN 11th HOUR CRISIS

AVOIDANCE: The worst option

- Ignore any concerns and hope that they will go away. They won't.

ACCOMODATION: and the other not-good options

- Project demands that Infosec allow them to release despite concerns.
- Infosec demands project holds off on release until all issues are resolved.

COMPROMISE:

- Project is allowed to release as long as the feature in dispute is disabled.

COMPETITION:

- Both sides commit resources to holding their line, without trying to bring the other side along with them.

COLLABORATION: The best option

Identify what the needs of both sides are and what options there are to manage the security risk and delivery risk that each party is concerned about.

CREATING CHANGES IN YOUR ORGANISATION

THE POINT AT WHICH YOU START THINKING ABOUT SECURITY MATTERS

ANALYSIS AND PLANNING

Risk can be **CONTROLLED**

PREVENTATIVE measures are possible.

(ie: secure-by-design application development)

DESIGN AND BUILD

Risk can be **MANAGED**

ADAPTIVE measures are possible.

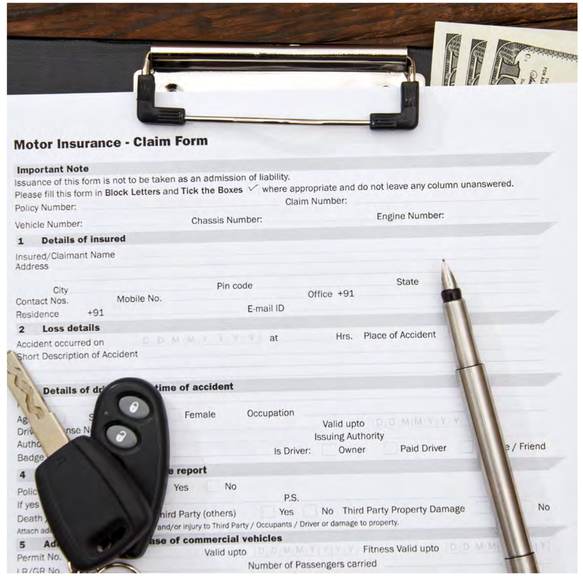
(ie: Deploying new firewall rules, access controls and malware filtering)

TESTING AND RELEASE

Risk can be **MEASURED**

Some **RESPONSIVE** measures are possible.

Such as: Incident response planning and Monitoring tools



IN SERVICE

Risk is **UNCONTROLLED**

Only **REACTIVE** measures are possible

ANY QUESTIONS?

TIME FOR A SHORT BREAK

Part 4

SHIFTING CYBER-RISK ANALYSIS TO THE LEFT

A LACK OF AIR TRAFFIC CONTROL

An SQL Injection Attack allowed a security consultant to bypass the access controls on a system for administering records of airline crew. This could have been prevented by coding input validation into the form.

"Using the username of ' or '1'='1 and password of ') OR MD5('1')=MD5('1, we were able to login to FlyCASS as an administrator of Air Transport International!"

Source: https://ian.sh/tsa

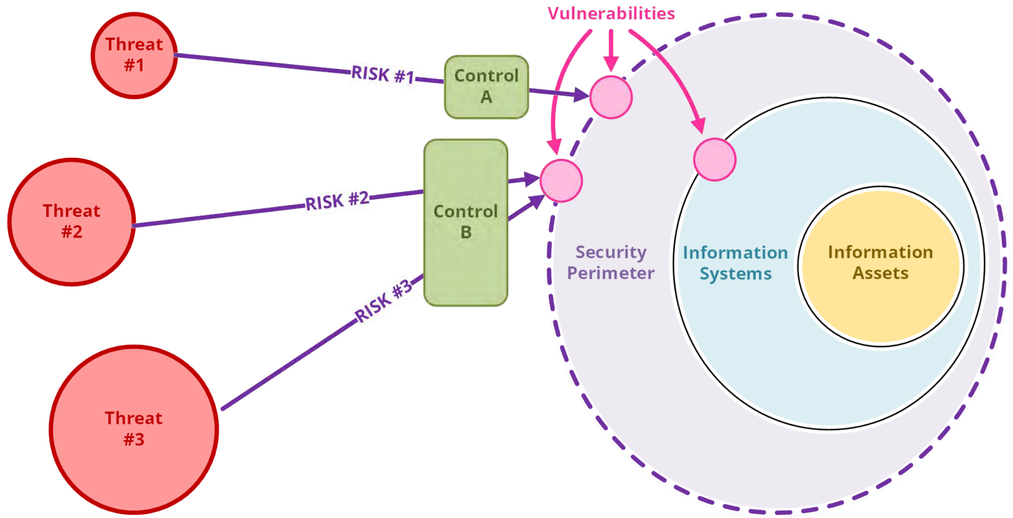
CYBERSECURITY TACTICS 101

ANATOMY OF A CYBER-ATTACK

Information Security is the practice of keeping information assets safe and secure within your SECURITY PERIMETER.

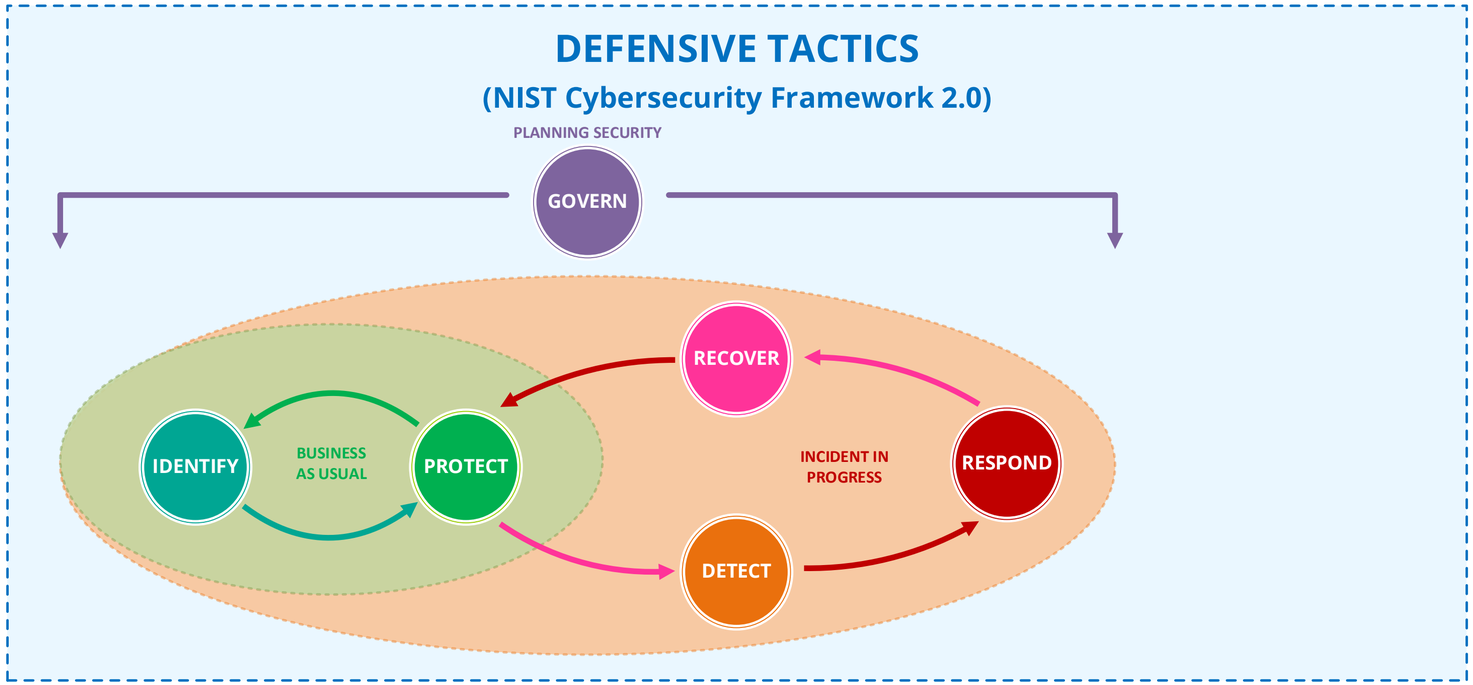
Design choices made during development can leave VULNERABILITIES in the final information system that can be exploited by a THREAT ACTOR (attacker).

This combination of a vulnerability and a credible threat actor represents a RISK that needs to be managed with a CONTROL.



These controls are usually organized within a framework that helps you to ensure that they provide comprehensive protection.

- The green controls are heavily involved in the change process.
- The orange controls are needed to manage the effect of a cybersecurity incident.
- The purple controls provide a degree of oversight across all other controls.



Source: https://www.nist.gov/cyberframework

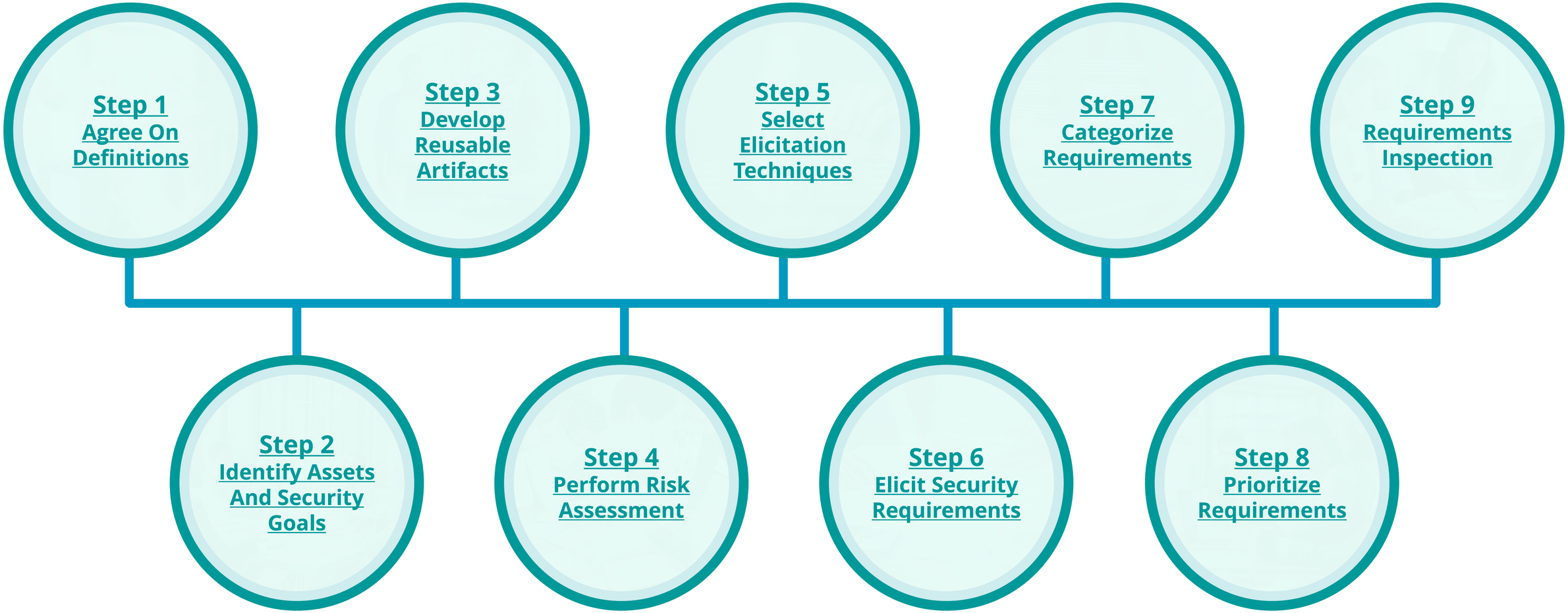
THE PERILS OF SECURITY DEBT

Security debt is the backlog of features and controls that would be required to protect your organization but haven't been implemented yet. These unresolved issues regularly provide opportunities for attackers while also creating more work for your organization.

The environment is likely to be more fragile, testing will take longer, and unauthorized access might be harder to detect.

INTRODUCING THE SQUARE FRAMEWORK

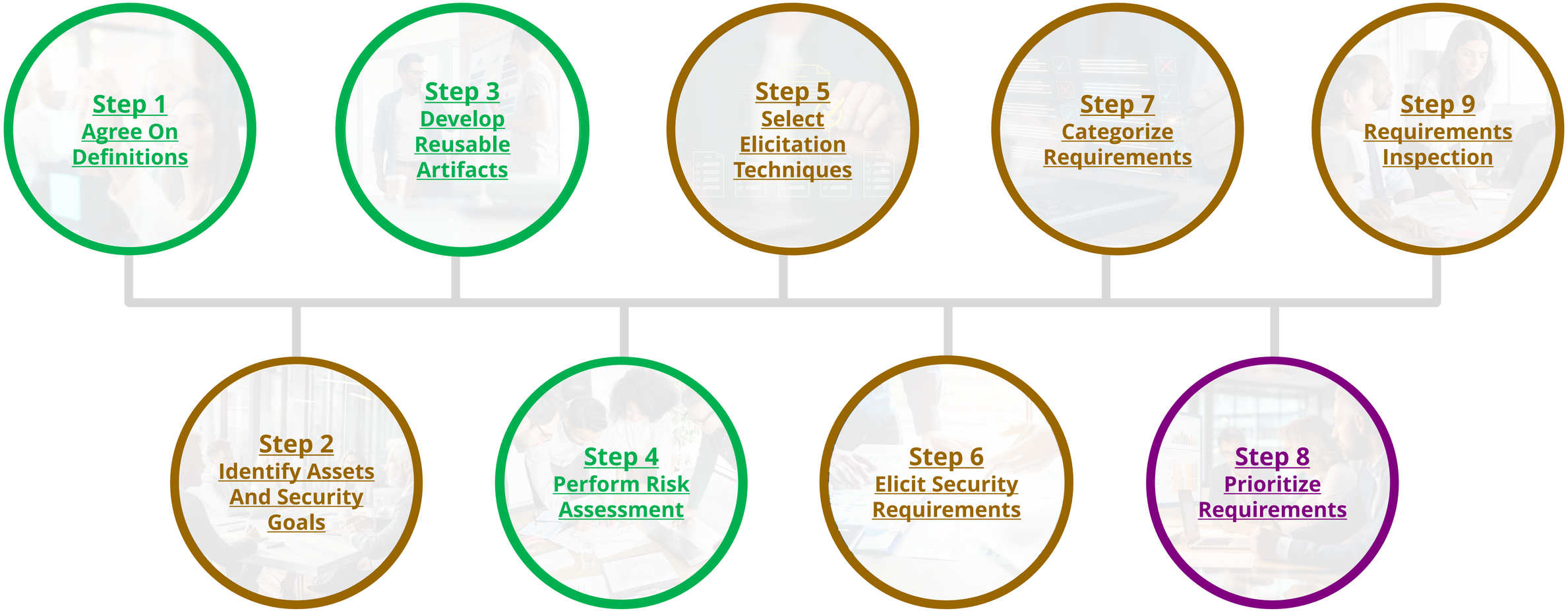
SECURITY & QUALITY REQUIREMENTS ENGINEERING



Source: https://insights.sei.cmu.edu/library/cybersecurity-engineering-research-security-quality-requirements-engineering-square-collection/

INTRODUCING THE SQUARE FRAMEWORK

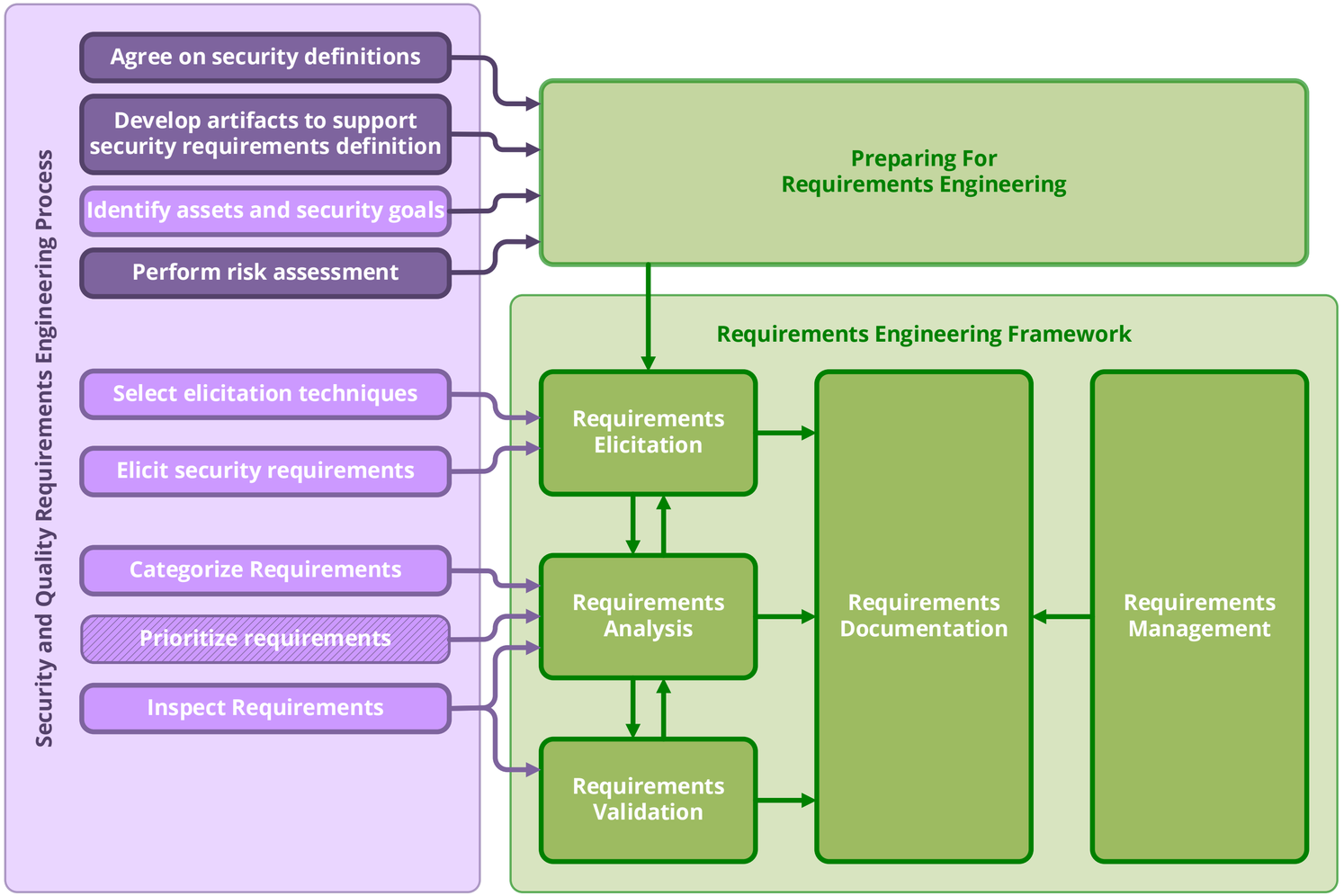
SECURITY & QUALITY REQUIREMENTS ENGINEERING



Source: https://insights.sei.cmu.edu/library/cybersecurity-engineering-research-security-quality-requirements-engineering-square-collection/

ALIGNING SQUARE TO OTHER MODELS

SQUARE aligns well with other models for conducting business analysis such as the Requirements Engineering Framework and the activities in the IIBA's Business Analysis Body of Knowledge v3.



RECOMMENDATION ONE

GET TO KNOW YOUR CYBERSECURITY FRAMEWORK

Your organisation has probably adopted a framework for organising their controls. Understanding this system helps you to identify potential impacts and communicate issues with infosec and change teams.

Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

RECOMMENDATION TWO

DEVELOP REUSABLE SECURITY ARTIFACTS

- Maintain a catalogue of reusable security requirements and acceptance criteria.
- Develop a set of “bad actor” personas to test design assumptions
- Identify appropriate Security SLAs and industry benchmarks

Useful Resources:

- https://www.cisecurity.org/cis-benchmarks
- https://www.cisecurity.org/controls/cis-controls-list
- https://owasp.org

QUICK PUBLIC SAFETY ANNOUNCEMENT

REMEMBER US WHEN YOU DEVELOP PERSONAS

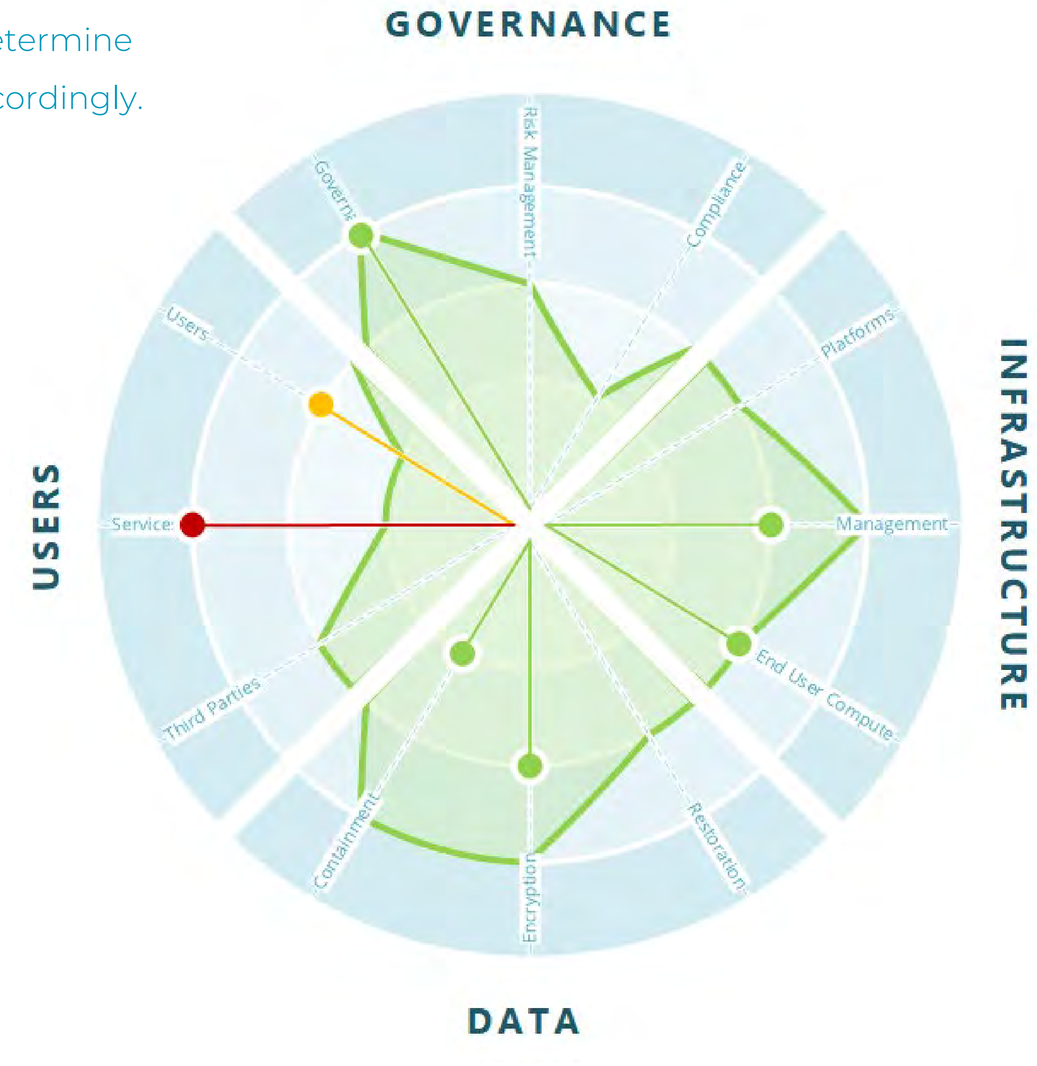
Motivated By An Ideology

Motivated By Financial Reward

RECOMMENDATION THREE

ASSESS PROJECT CYBER-RISK EARLY

Make sure that you can identify the security impact of your project, so that you can determine what the key risk factors are and consult or inform your information security team accordingly.



RECOMMENDATION FOUR

ENSURE PRIORITISATION IS INFORMED BY RISK

Most of the time, the prioritisation of new project deliverables is based on the value that a new feature would deliver and the effort/cost of developing it.

This is good for delivering functionality, but it ignores the importance of ensuring that the capabilities that you deliver is secure and resilient and doesn't compromise any other systems.

It is good practice to try to assign a rough value for risk as well to give you more accurate priorities.

$$\frac{\text{VALUE DELIVERED}}{\text{DEVELOPMENT + COST OF CYBER-RISK}}$$

$$\text{COST OF CYBER-RISK} = \frac{\text{TOTAL VALUE OF ASSETS x \% OF VALUE AT RISK}}{\text{PROBABILITY OF LOSS IN ANY GIVEN YEAR}}$$

SOME FURTHER READING...

- NCSC (UK) Cybersecurity Assurance Framework
  https://www.ncsc.gov.uk/collection/cyber-assessment-framework
- https://www.ncsc.gov.uk/collection/cyber-assessment-framework/terms-and-definitions
- Cybersecurity Body of Knowledge (UK) – Advanced
  https://cybok.org/media/downloads/CyBOK_v1.1.0.pdf
- NIST (US) Cybersecurity Framework
  https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- CISA (US) Secure By Design Principles
  https://www.cisa.gov/securebydesign
- CISA (US) Zero Trust Maturity Model
  https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

ANY QUESTIONS?

Thank Your For Your Participation

Connect with me
on LinkedIn at:
WWW.LINKEDIN.COM/IN/MARKCROSS

BUSINESS ANALYSIS CONFERENCE EUROPE

16 - 18 September 2024 • London, UK

Please score and comment on this session and speaker in the event mobile app

IRMUK