The $10.5 Trillion Cyber Threat: Incident Strategies for Survival

Dr Clive King; Conor Horgan

If measured as a country, Cybercrime would be the world's third-largest economy after the U.S. and China (Cyber Crime Magazine, April 2024). It was predicted to inflict damages totalling $10.5 trillion globally in 2025 — that is averaging around $350 for each of the 29 billion internet connected devices. This white paper discusses the scale and inevitability of cybercrime, the increasing compliance demands from DORA and NIS2 regulations and offers three strategies to respond more effectively to them and enhance your current prevention approaches: 1) Incident Mapping to identify and strengthen your cyber vulnerabilities 2) "4-colour thinking" to manage your cyber-incident bridge with more clarity 3) Engineering your Performance System to make your Cyber Strategies work.

Background & Context

KT & Cybersecurity

IT security should be a primary concern for every individual and business, large or small. The threats are pervasive, evolving and relentless. This white paper considers how the *Kepner-Tregoe (KT) Clear Thinking Process* may be applied to the field of IT security. It is not a manual, but a set of pointers for those trained (or interested) in KT process to apply to the field of computer security. We don't claim to be a full-service cyber partner. However, we are experts in many of the transferable skills, behaviours and processes that underpin an effective proactive and reactive cyber response. If cyber security is a 500-piece jigsaw board, we are the 4 key corner pieces which help you set the rest in context.

KT consultants are highly experienced in applying KT's clear thinking methods to complex and evolving business problems. Today, business has no greater and more rapidly evolving challenges to deal with than those associated with cybersecurity. A holistic approach to cybersecurity means strengthening tools, administration procedures and, critically, problem solving / decision making / risk management processes.

Cybersecurity is extremely challenging because:

1. The threat landscape is continually evolving.
2. Technical experts, compliance and governance staff, human factors experts and decision makers often don't understand each other, don't speak the same language and may have conflicting priorities.
3. Accountants, regulators and sales pressures direct or constrain resources in ways unrelated to the scale and nature of actual threats.
4. The adversary(s) are well resourced, often beyond legal reach and with the morals of a street gang.
5. In aggregate, as an industry, IT does not care nearly enough about cybersecurity and puts backward compatibility as its top priority[1]. Would SQL (injection attacks) and Excel macros still exist as attack vectors if the industry really cared about security attack vulnerabilities?
6. The attack surface is huge, and users often have little effective control over the security profile of the operating systems, network infrastructure and application stack they run.
7. It is expensive and error prone work to keep up to date with software versions, patches, network configurations, credential permissions, password quality and retirement, etc.

Cybersecurity is a highly cerebral and communal activity covering the whole spectrum of computer science, human psychology, physical security, criminology and much more. Situations are often unique, combining high levels of uncertainty with high business impact and consequences. The best engineers and managers benefit from having their problem solving and creative skills enhanced with a common process and language. For the less experienced, the benefits to productivity are even greater. Resource allocation in the fight against cybercrime is highly skewed to product and process, typically far less is allocated to training and improving the quality of thinking of the defending side. This is a major gap.

Since the late 1950's KT has brought clear thinking to complex situations across the whole spectrum of business and wider human endeavours (getting Apollo 13 safely home, for example). Its methods have been shown to be highly effective within the most complex IT environments and the value chains they support. Cybersecurity is no different in its need for effective and repeatable thinking patterns to be applied to its incidents and challenges. KT process is the HOW that ties together the need to deliver business value with technical knowledge and skills,

[1] If today you were going to architect a language to promote the spread of malware, it would look like the 39 year old language PostScript. It has only just been removed by default from Windows and OSX in 2023. LM hashing in Microsoft Lan Manager (1987) compatibility mode still exists in modern Windows versions.

effective governance and people management, in order to plan effective action to prevent and mitigate cybersecurity threats.

KT process can be used standalone or to provide strategic direction and input for techniques such as formalized security methods like threat modelling, NIST audits and penetration testing.

New Era of Cyber Security: The Era of Compliance

2024 has been dubbed a new era in cyber security – 'the era of compliance' by Sounil Yu, a highly respected cyber-security expert. This is a result of the rollout of the Digital Operational Resilience Act (DORA) and the second phase of the Network and Information Security Directive (NIS2). These regulations now represent huge changes to EU operational organisations' cyber strategies.

The Five Pillars of DORA are shown below. What stood out to us ahead of our itSMF Conference talk in November 2024 were the following:

- We must be better at identifying and managing the risks.
- We have more reporting milestones to consider as Incident Managers.
- We must ensure that we're sharing our threat intelligence effectively, now it's mandated.
- We need to have a strong post-mortem defence aligned to these Five Pillars and that requires our decision-making rationale to be traceable.

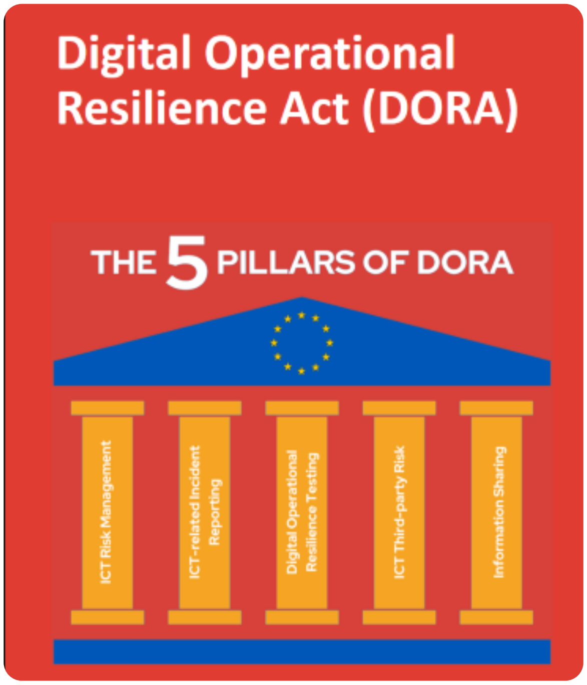

Digital Operational Resilience Act (DORA)
THE 5 PILLARS OF DORA
ICT Risk Management
ICT-related Incident Reporting
Digital Operational Resilience Testing
ICT Third-party Risk
Information Sharing

Figure 1:
Pillars of DORA taken from Continuity2.com

In relation to the NIST Cyber Security Framework Core (see image below) KT is best known for operating in the 'Respond' space with our Major Incident Management approach. NIS2 was rolled out in October 2024 and mandated that organisations communicate their incidents more frequently:

- **Within 24 hours:** must notify the authority that you have been hacked
- **Within 72 hours:** must contact and update the authorities
- **Within 30 days:** you must conclude investigation with authorities

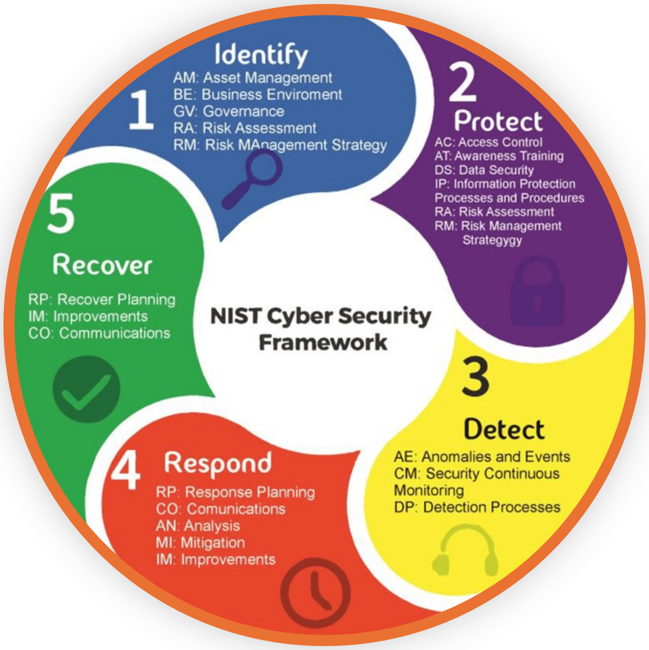


Figure 2: NIST Cyber Security Framework core taken from SEP.com.sa

So, what does this mean for Major Incident Managers and bridge calls? Well, there's extra pressures, stakeholders, deadlines and complexities to manage.

Fight or Flight Chaos in the Eye of the Cyber-storm

Over the past year, we've asked 'what are the biggest challenges to effective Major Incident responses?'. The main responses we received are:

- Setting & controlling changing priorities
- Lack of visibility – complexity of tech increasing
- Communicating expectations
- Providing satisfactory status updates to various stakeholders
- Managing involvement (of 3rd parties)
- Pressure – chaos vs. calm required
- Bridge dilution – technical vs. management

- Too much noise in too many (technical / national) languages

Major Incident Managers have communicated to us that they feel increasingly stressed and under pressure. However, now consider some extra elements of a Cyber Major Incident that heighten the above:

- Public Relations (PR) impact of data held ransom (across supply chain including end users and clients).
- Additional compliance milestones and requirements (NIST2 & DORA).
- Insurance updates to ensure you are following every procedure to validate your claim.
- A potentially novel scope of scale of issue.
- More partners for recovery (internal & external) including law enforcement and ransom criminals themselves.

If Major Incident Managers feel stretched, stressed, and under pressure currently, Cyber Incidents are a whole new level of complexity and intensity, demanding even more advanced skills, rapid response, and comprehensive coordination under the most extreme pressure.

Extensive research over the past 20 years explains how when pressure is applied, the thinking part of our brains shut down – we revert to fight or flight responses. A new study has found a link between stress and reduced cognitive function. People were 37% more likely to have lower cognitive function when they had elevated stress (Source: JAMA 2023). Major Incident Managers and teams operate in this high-pressured space. Along with useful strategies for mental health, robust processes, behaviours and performance systems can be relied on to help Major Incident Managers think clearly in chaos.

Three Strategies to Consider

1) Manage the Bridge by separating our 4 basic thinking patterns

Research from the KT founders Charles Kepner and Ben Tregoe (https://kepner-tregoe.com/app/uploads/2024/03/The-New-Rational-Manager-new-cover-chapters-1-and-4.pdf) highlighted how there are four basic thinking patterns that have not altered much since the emergence of humanity:

1. **What's going on?**
2. **Why did that happen?**
3. **What course of action should I take?**
4. **What lies ahead?**

Almost all productive activity in your organisation is related to one of these four basic thinking patterns. Whilst we all use these patterns of thinking consciously or unconsciously, our client observations over 65 years have made us conclude that many organisations are inefficient in this respect and do not perform in high pressure scenarios because they try to do these at the same time – they lack clear thinking. This is particularly noticeable on Major Incident bridges.

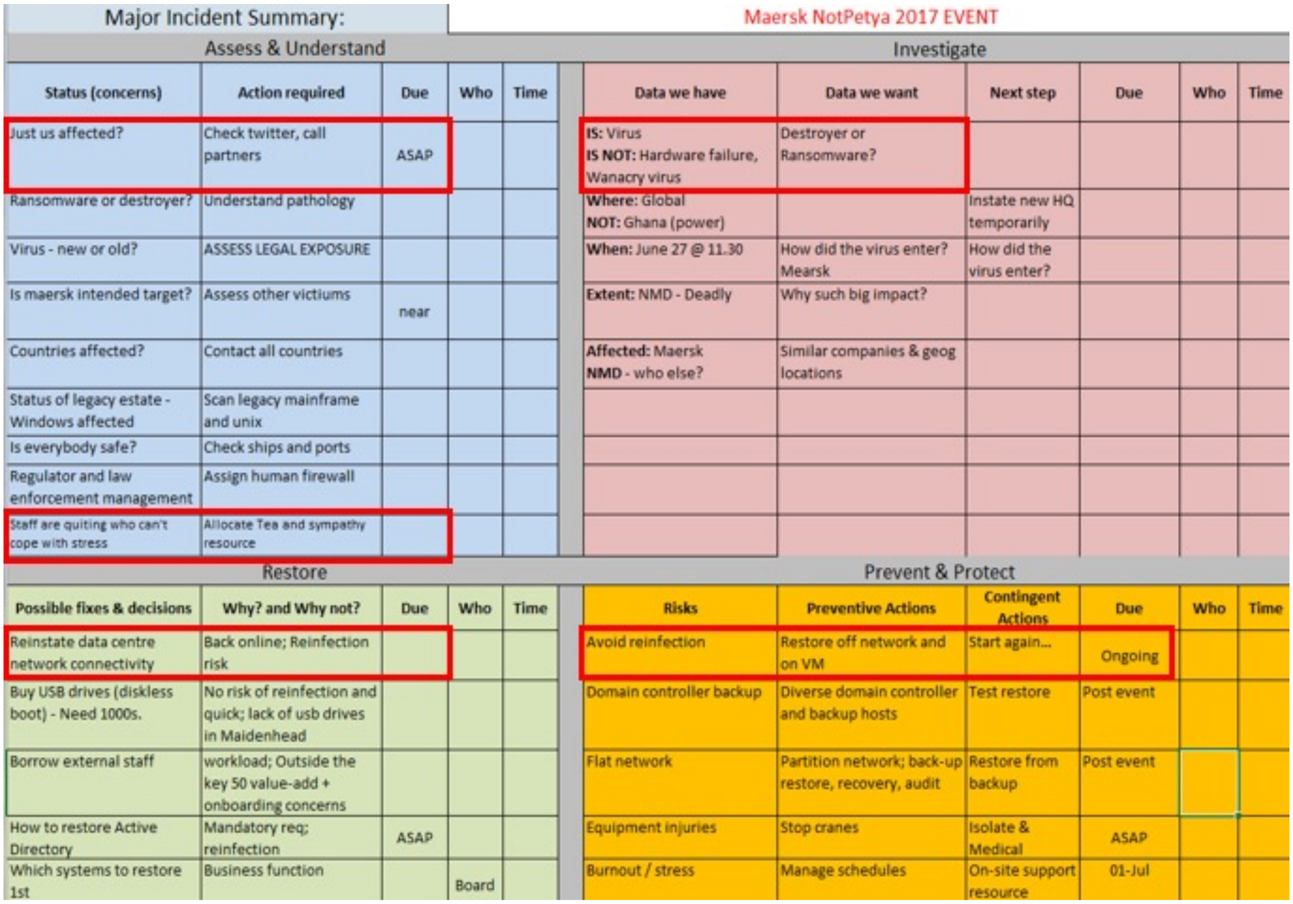
Separation is key – multi-tasking is a myth. For each of these thinking patterns, our founders created systematic processes for making the best possible use of your 4 patterns of thinking, to be worked one at a time:

What's going on?	**Situation Appraisal**
Why did that happen?	**Problem Analysis**
What course of action should I take?	**Decision Analysis**
What lies ahead?	**Potential Problem Analysis**

When Major Incident Managers separate the bridge communication into these four colours, made visible to all bridge attendees, it enables clarity in chaotic and complex situations. The MIM can better orchestrate the meeting by keeping people in the same box. For example, when asking initial assessment questions and for initial concerns, the team are directed to provide data for the blue box rather than bounce chaotically between **restoration options,** **theories of cause**, **potential risks** and getting more **understanding of the current situation.**

Below is an example of how a Major Incident might have been made visible during a bridge during the Maersk NotPetya cyber attack in 2017 constructed from publicly available sources (https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world). NotPetya was nation state actor grade malware for which Maersk was not the intended target. Substantial IT infrastructure which ran the largest shipping company in the world and supports a significant subset of global shipping trade was taken offline for 10 days and took 6 months to fully recover. Separating the concerns, actions, decisions and risks into 4 colours allows us to think clearly in times of extreme stress. Below is a simplified example of a subset of the issues that Maersk may have had to deal with early in the lifecycle of the attack.

When presented with this template in a class, one of our clients, at lunch time, printed A0 empty copies of this template to stick on a wall in the event that they lost power or access to computers and to be able to manage the early stages of a major incident on paper if required.



Major Incident Summary:

Maersk NotPetya 2017 EVENT

Assess & Understand

Status (concerns)	Action required	Due	Who	Time
Just us affected?	Check twitter, call partners	ASAP		
Ransomware or destroyer?	Understand pathology			
Virus - new or old?	ASSESS LEGAL EXPOSURE			
Is maersk intended target?	Assess other victiums	near		
Countries affected?	Contact all countries			
Status of legacy estate - Windows affected	Scan legacy mainframe and unix			
Is everybody safe?	Check ships and ports			
Regulator and law enforcement management	Assign human firewall			
Staff are quiting who can't cope with stress	Allocate Tea and sympathy resource			

Investigate

Data we have	Data we want	Next step	Due	Who	Time
IS: Virus **IS NOT:** Hardware failure, Wanacry virus	Destroyer or Ransomware?				
Where: Global **NOT:** Ghana (power)		Instate new HQ temporarily			
When: June 27 @ 11.30	How did the virus enter? Mearsk	How did the virus enter?			
Extent: NMD - Deadly	Why such big impact?				
Affected: Maersk **NMD** - who else?	Similar companies & geog locations				

Restore

Possible fixes & decisions	Why? and Why not?	Due	Who	Time
Reinstate data centre network connectivity	Back online; Reinfection risk			
Buy USB drives (diskless boot) - Need 1000s.	No risk of reinfection and quick; lack of usb drives in Maidenhead			
Borrow external staff	workload; Outside the key 50 value-add + onboarding concerns			
How to restore Active Directory	Mandatory req; reinfection	ASAP		
Which systems to restore 1st	Business function		Board	

Prevent & Protect

Risks	Preventive Actions	Contingent Actions	Due	Who	Time
Avoid reinfection	Restore off network and on VM	Start again...	Ongoing		
Domain controller backup	Diverse domain controller and backup hosts	Test restore	Post event		
Flat network	Partition network; back-up restore, recovery, audit	Restore from backup	Post event		
Equipment injuries	Stop cranes	Isolate & Medical	ASAP		
Burnout / stress	Manage schedules	On-site support resource	01-Jul		

Figure 3: MIM Dashboard example of the Maersk NotPetya 2017 event made by Dr Clive King (Kepner-Tregoe)

2) How you visualise things makes a big difference

The four colour dashboard approach during a bridge call highlighted the importance of making your team's thinking visible, effectively, to achieve clarity in chaos. When looking to identify your cyber risks and vulnerabilities, the same message applies – how you visualise it makes a significant difference.

Many Post Incident Reviews, Cyber Security Plans, matrices and assessments that we have seen share the same limitations when trying to identify and manage their cyber vulnerabilities:

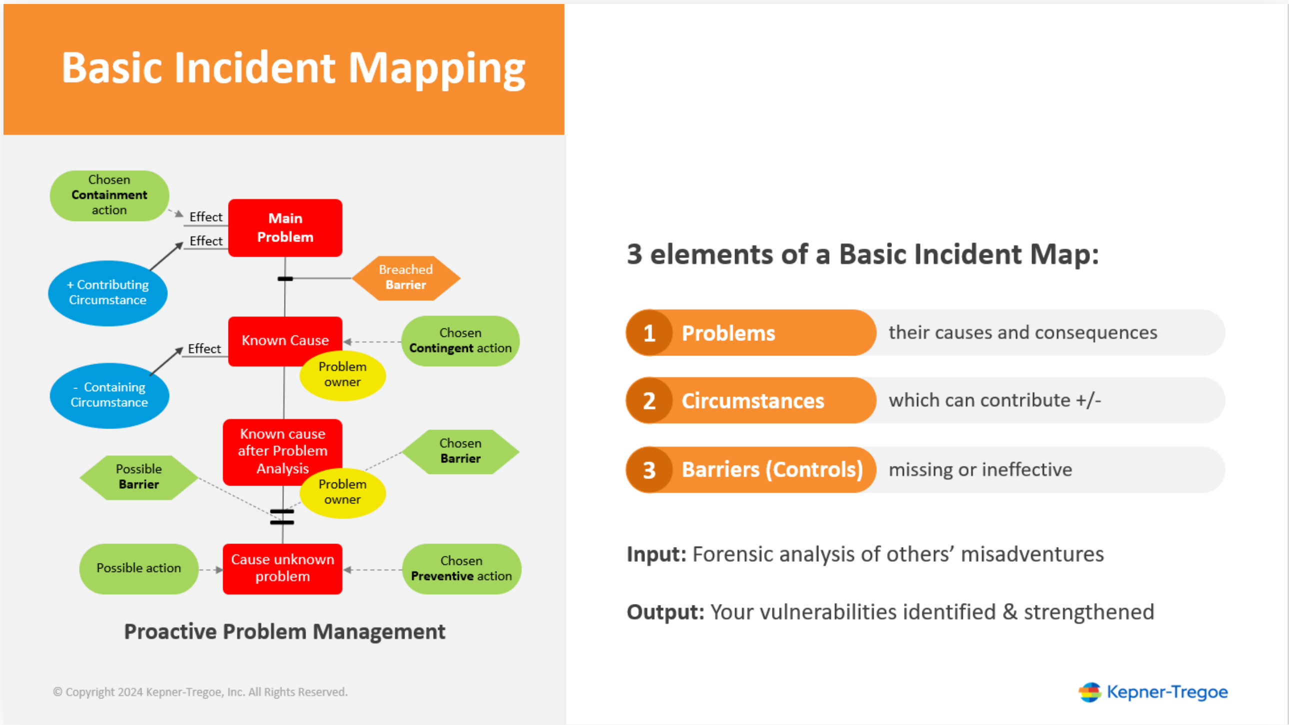
1. They are **'zombie documents'** – by which we mean they are not 'live'. They are not quickly and easily digestible to encourage effective contributions and improvements.
2. The **rationale is hidden, missing or buried** – this makes it difficult to effectively challenge their underlying assumptions.
3. The **rationale is one-dimensional** – it is cause and effect based, often zoned in on the technical vulnerabilities and missing a clear separation of contributing circumstances and ineffective or missing controls.

Whether it is learning from other organisation's misfortunes or visualising the outcomes of your DORA-mandated penetration tests, Incident Mapping can address these three limitations.

Incident Mapping

Incident Mapping is a highly visual live document which teams can digest easily and therefore contribute to quickly. It has scalable organisation-wide potential and has tangible results by quantifying the improvements you make to your cyber defence to management and the organisation.

The three basic elements of an Incident Map are shown below:



Basic Incident Mapping

Proactive Problem Management

© Copyright 2024 Kepner-Tregoe, Inc. All Rights Reserved.

3 elements of a Basic Incident Map:

1. **Problems** their causes and consequences
2. **Circumstances** which can contribute +/-
3. **Barriers (Controls)** missing or ineffective

Input: Forensic analysis of others' misadventures

Output: Your vulnerabilities identified & strengthened

Kepner-Tregoe

Figure 4: Three basic elements of an Incident Map, by Kepner-Tregoe

1. **(Technical) causal chain** – working back from the problem to its direct (technical) causes i.e. the technical vulnerability in your system responsible for the breach
2. **Contributing circumstances** – that made you more or less vulnerable to attack
3. **Breached/Missing Barriers** – i.e. missing or ineffective monitoring or controls that should have been protecting your vulnerabilities

The moment you visualise the (potential) incident in this format, it instantly transforms into a continuous improvement exercise. It provides you with the opportunity to:

1. Eliminate your technical vulnerabilities
2. Introduce more effective controls to strengthen and protect your vulnerabilities
3. Plan more worst-case scenarios

These can drive effective metrics to measure the effectiveness of your cyber planning that can be easily communicated with all levels of your organisation, in addition to providing a dopamine hit to the team conducting the work.

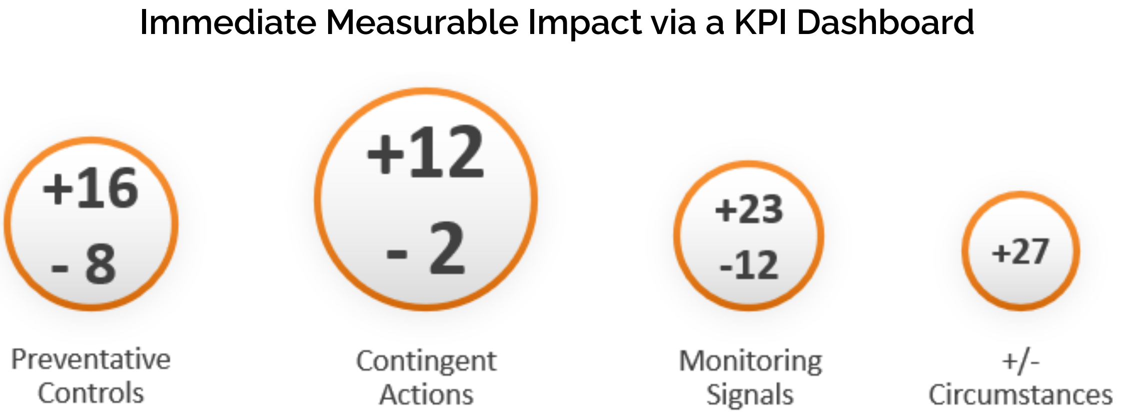


Figure 5: Illustration of potential Incident Mapping dashboard showing (+) improved actions taken and (-) ineffective actions removed

These improvements can be made by going down the causal chain and identifying and addressing your vulnerabilities, the causes of the (potential) attack. However, Incident Maps can also be used to foresee and better manage the effects that your Major Incident Manager and teams would likely be left to grapple with.

By going 'up' from the problem, you can foresee the likely effects of the (potential) attack that you must manage. These can be categorised into your main organisational measures, or the main considerations you should consider in the event of an attack. Six are suggested as an example in **purple**, below.

Earlier we discussed the need to have clarity in the chaos of the cyber storm – having pre-planned contingencies to effectively manage the effects provides you with that, even with simple "if x, then y" thinking or by using Potential Problem Analysis.

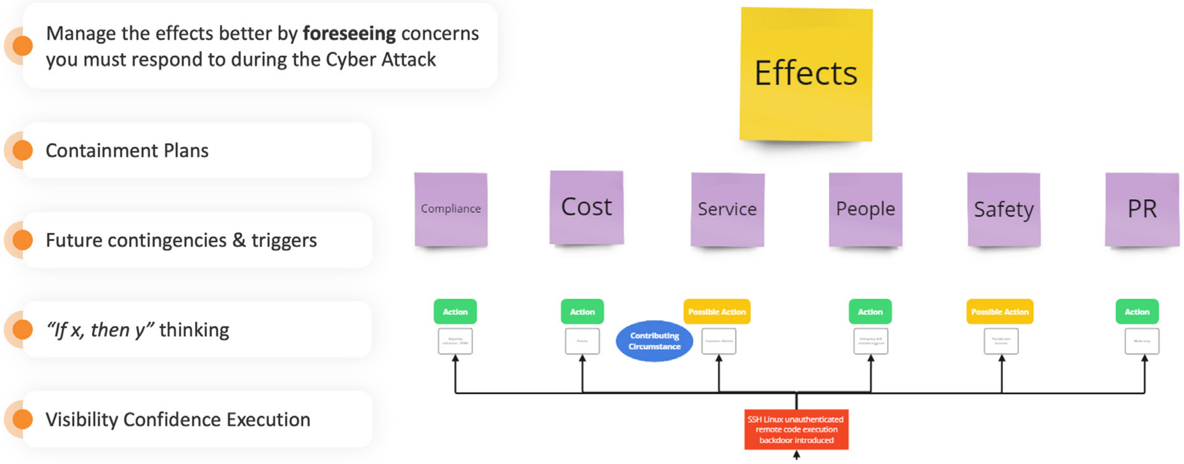

Manage the effects better by **foreseeing** concerns you must respond to during the Cyber Attack
Containment Plans
Future contingencies & triggers
"If x, then y" thinking
Visibility Confidence Execution
Effects
Compliance
Cost
Service
People
Safety
PR
Action
Action
Contributing Circumstance
Possible Action
Action
Possible Action
Action
SSH Linux unauthenticated remote code execution backdoor introduced

Figure 6: Example of how you can visualise the (actual/potential) effects of the cyber-attack to manage the effects

XZ Supply chain attack 2024 Example

Below is an example of how we can learn from others' unfortunate events. The XZ supply chain attack in February 2024. We put this together based on the information produced by Thomas Roccia in Security Break[2] – this is not a client case study.

The XZ Supply Chain attack is interesting not only because of its complexity, but also that a person of unknown identity spent 18 months gaining trust in the Open-Source community to insert an attack vector into a key Linux component.

The type of attack may be a leading indicator of the types of attacks to come, both in Open and Closed source environments.

The red boxes show the causal chain, asking "why?" for each cause until we can no longer make progress.

The hexagons are barriers or controls which have been breached and the blue ovals are circumstances which contribute to each cause.

The circumstances can also be thought of as business decisions which have been made, either explicitly or have evolved organically over time.

The incident map represents an effective way to communicate very complex post incident reviews, with both the causal chain and remediations being made clear on one page.

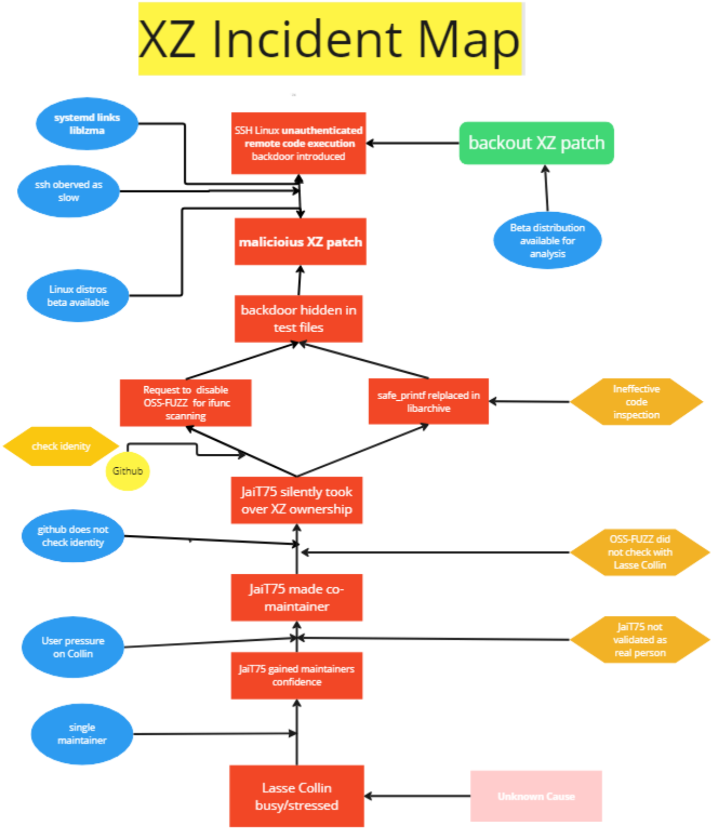

XZ Incident Map
systemd links liblzma
SSH Linux unauthenticated remote code execution backdoor introduced
backout XZ patch
ssh oberved as slow
malicioius XZ patch
Beta distribution available for analysis
Linux distros beta available
backdoor hidden in test files
Request to disable OSS-FUZZ for ifunc scanning
safe_printf relplaced in libarchive
Ineffective code inspection
check idenity
Github
JaiT75 silently took over XZ ownership
github does not check identity
OSS-FUZZ did not check with Lasse Collin
JaiT75 made co-maintainer
User pressure on Collin
JaiT75 not validated as real person
JaiT75 gained maintainers confidence
single maintainer
Lasse Collin busy/stressed
Unknown Cause

Figure 7:
XZ Supply chain attack 2024. Cyber-attack visualised using an Incident Map, by Clive King (based on information from Thomas Roccia in SecurityBreak - https://blog.securitybreak.io/security-info-graphics-9c4d3bd891ef

[2] https://blog.securitybreak.io/security-infographics-9c4d3bd891ef

3) Making your Cyber Strategies Work: Effective Governance

In this white paper we have suggested two main ways to improve your cyber strategies: 1) managing the bridge communications in four colours and 2) incident mapping to strengthen and protect your cyber vulnerabilities. You will have many strategies that should in theory protect you against some attacks or make you more resilient in the event of the inevitable successful attack. However, how do you shift gears from a plan to effective action? The answer lies in the governance.

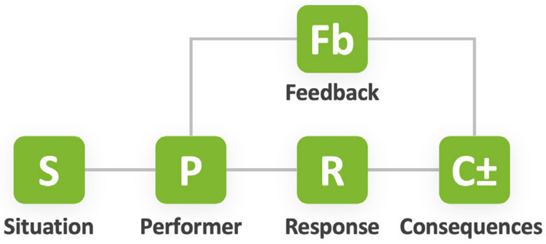
Too often organisations pay lip service to cyber defence and rely on their employees doing cyber security training to prevent effective phishing attacks. Training alone does not give anyone the confidence to successfully execute anything. Training alone does not make the difference, it's the employee behaviour. You can engineer your Performance System (the environment within which your employees do their work) to encourage the desired behaviours and therefore increase the probability of cyber strategy effectiveness.

Phishing emails are the number one vector of successful cyberattacks, so how effective is your organisation's strategy to prevent it? In another white paper we are producing in 2025, we will discuss the importance of Engineering the Human Performance System in more detail, but below we will provide a short example of how you can engineer the Performance System of your phishing email strategy and make your training more effective.

Engineering the performance system gives us crucial insight rooted in the perspective of the performer. The world view of the performer is often dramatically different to those trying to direct change. When we engineer the performance system with clients to sustain behavioural change, we separate the performers to consider:

1. the user
2. the management
3. the coaches who may be tasked with ensuring consistent capability development.

The graphic below shows the steps in our Performance System, with a sample of some of the questions to consider at each stage.



Step	Questions
Situation	How clear are the performance expectations? How well does the work environment support it? How clear is the signal to perform?
Performer	How capable are they to meet the performance expectations?
Response	What is the observed response? How does it compare with the expectations?
Consequences +/-	How well do they encourage expected performance?
Feedback	How appropriate is it? How well is it used to influence performance?

Figure 8: Visualisation of Kepner-Tregoe's Human Performance System and sample questions to ask at each stage

When using this tool to strengthen the effectiveness of your phishing email strategy, here are some points to consider at each stage:

1. **Situation:**
   - Training can be mandatory.
   - You can use Potential Problem Analysis to increase attentiveness and effectiveness of training modules e.g. cannot be watched with no sound or fast-forwarding.
   - Monthly Executive Report to include section on cybersecurity and phishing strategy.
   - Introduce simulated attacks and training to clearly explain how to respond to any potential phishing email by clicking the phishing button and reporting it to IT.
   - Communicate importance of phishing response at every management level.
   - Easily accessible KPIs showing your organisation's, teams' and individuals' performance.
2. **Performer:**
   - All employees to have a phishing button and be capable of using it.
   - Training to be short in length to fit into workloads and at acceptable frequency, e.g. monthly modules.
3. **Response:**
   - Easily accessible visibility of the performer's response from training modules, simulated attacks and successful phishing reports sent.
4. **Consequences:**
   - Leaderboards in company-wide reporting phishing by email, monthly CEO update and quarterly review.
   - Remove short term negative consequences, e.g. being talked to for incorrectly flagging a potential phishing attack.
5. **Feedback:**
   - Peer pressure from the leaderboard's visibility will be a natural driver.
   - Consider including your phishing response in performance reviews, including ones linked to performance related appraisals.

The above is an example of how you can better engineer your performance system to make your cyber training more effective. However, it is not bulletproof.

There must be a balance of acceptable risks and consequences. For example, one way to eliminate the chance of a CEO clicking on a phishing link is to disable that function from all their emails. However, that would be impractical in terms of how they perform their job. Therefore, you might have to accept a level of risk and certain consequences to balance your organisation's health and performance.

Summary

1. So we all need to wake up to the size of the $10.5 trillion cyber threat, the extreme chaos it brings, and its inevitability owing to our legacy infrastructure. Executive Directors are seeing this increasingly as a key organisational priority, so use this moment to speak up about your legacy vulnerabilities, even more important in this era of compliance.
2. Map it to make it happen - consider engaging visualisations of (potential) incidents to increase your controls, detection and resilience in the storm, alongside any ethical hacking you may do, especially since mandated in DORA.
3. In the eye of the cyber storm, you will need to make some of the biggest decisions of your career, such as whether to pay the ransom to secure your data. Your ability to think clearly will be naturally impeded by the pressure you will be under. In addition, together with partnering with a good insurer to help guide you during the attack, practice strategies to think clearly in chaos before the inevitable attack arrives. Make objective, rational decisions now that you can rely on, or at least make the frameworks visible so that you have rational thinking processes to enable clarity in chaos.
4. Shift gears by making your cyber strategies work – ask how effective your performance system is at encouraging the desired behaviours. Start small – what can you do tomorrow to improve the effectiveness of your phishing email training?
5. Share, share, share! NIST2 and DORA are built on the premise that we should be working as a community against cyber criminals. Learn from others' misfortunes and near misses. When it comes to sharing your threat intelligence, share with the intent for others to effectively contribute and improve it. For example, what if you presented an incident map at a conference and made it participative with the audience? That way all parties benefit in this battle against the cyber criminals.

Share your thoughts with us:

Dr Clive King cking@kepner-tregoe.com

Conor Horgan chorgan@kepner-tregoe.com