As the boundaries between physical and digital realms blur, **the ability to anticipate and respond to cyber has become critical to bolstering organizational resilience**

Introduction

If any part of a business involves being connected to the internet, it automatically becomes susceptible to a cyber attack. Such a threat has become so commonplace that it is an 'accepted part of life', yet with that acceptance comes a dangerous form of complacency. It has become all too commonplace to turn to cybersecurity to protect your business interests, yet that action in itself makes one potentially fatal supposition – that any implemented cybersecurity measures will be 100% effective.

We have a slight problem in that one of the most common means of hacking a company comes through members of staff failing to understand and adhere to cybersecurity protocols.

This then leads to a compounding of the problem – what to do when there is a security breach.

Consequently, this paper looks to explore the need for businesses and organisations to anticipate a crisis (be proactive).

How to make 'cyber' feel more 'real' in order to provide peace of mind

Company owners and CEOs are not cybersecurity experts. Consequently, when a CISO or head of cybersecurity in a company advises that all appropriate measures are in place to defend against cyberattacks, there is every likelihood they will be met with the question: "But what if?". Trying to reassure senior executives that their business is safe from a cyberattack will never wash as they do not have the knowledge to understand that cybersecurity measures in place will be effective. Instead, to provide peace of mind, the answer most executives will be looking for is a positive response explaining what will happen in the event of a 'successful' cyberattack, what measures and strategy are in place that will provide reassurance the business will still remain sufficiently protected, regardless.

It is like constantly imagining that if someone were to come up to us and attack us, we could defend ourselves. As the World Champion heavyweight boxer Mike Tyson famously said, "Everyone has a plan until they get punched in the mouth." Unfortunately, at some point, we are going to get punched in the mouth; it is how we react that matters more than anything. While we may attempt to protect ourselves effectively, mainly through training, effective cybersecurity comes from preparing to be punched and learning how to respond effectively.

How do we go about preparing for a potential crisis? First, start with a checklist:

- **Practice real-life scenarios. Stage simulated cyberattacks and potential scenarios, and allow the team to hone reactive skills essential for a positive outcome. The more you practice, the more you remove luck from the equation.**
- **Create strategies that are adaptable. Cyberthreats evolve over time, and you need a strategy that is flexible and adaptable, as opposed to creating a new strategy for ever new form of cyberattack.**
- **Identify potential and existing weaknesses by talking to people who inhabit the cybersecurity sphere and absorb what they have to say. Here it is suggested that ethical hackers as well as fellow colleagues, CISOs, etc., be included on the list. Apart from the fact they are more up to date than any written information or technical updates, talking to those who have intimate knowledge of the nature of problems faced helps to make everything feel more real.**
- **Establish effective interfaces with internal and external collaborators, including cybersecurity experts and appropriate authorities, to ensure that there is clear and efficient communication in a crisis.**
- **In the same way that hotels run fire drills and firefighters continually practice drills under emergency scenarios, why should it be different for cybersecurity? Running regular tabletop exercises[1] and full-scale 'incidents' not only allows you to become proficient when the 'real thing' happens, but it also allows you to identify any inherent weaknesses in procedures and protocols.**
- **It is important that all the training and exercises do not create a 'one-size-fits-all' approach to a crisis. Yes, there must be a general plan of action, but training should encourage flexibility and adaptability. Clear communication should mean that individuals turn to their superiors for help, guidance and constant discussions, rather than turning to a checklist of actions to be gone through step by step.**

1 https://www.researchgate.net/profile/Linas-Bukauskas/publication/320244434_Environment_for_Cybersecurity_Tabletop_Exercises/links/59e1336caca2724cbfdb73a0/Environment-for-Cybersecurity-Tabletop-Exercises.pdf

The plan of action

This can be carved up into three unequal sections where crisis management is concerned: preparation, prevention, and deliberate de-escalation.

95% Preparation – building up an effective barrier against cyberthreats and a state of 'readyness' requires continual preparation, primarily toward understanding the particular nature of threats, and the actions to be taken when detected.

4% Acute prevention – the development of a rapid-response culture and an ability to be agile. Constant monitoring and the ability to instantly neutralize an identified threat are essential.

1% Deliberate de-escalation – the deployment of specific strategies aimed at de-escalating a threat and minimizing direct and collateral damage are key. Structured decision-making and effective teamwork are crucial.

Because the working environment can be particularly stressful at times it is vital that the mental health and wellbeing of all team members be regularly assessed and appropriate action taken when needed. Emotional resilience is extremely important and the personal effect of a cyber attack on team members needs to be understood in order to optimize the efforts in crisis management.

The above is intended to help create an anticipatory culture within the cybersecurity environment[1].

Cyber resilience: embracing continuous agility

The definition of agility in cyber security is: "The property of a system or an infrastructure that can be reconfigured, in which resources can be reallocated, and in which components can be reused or repurposed so that cyber defenders can define, select, and tailor cyber courses of action for a broad range of disruptions or malicious cyber activities."

As organizations navigate the dynamic realm of cybersecurity, the imperative for continuous and agile improvement is paramount. Our insights from physical security and the adaptation of safety frameworks could set the foundation for an anticipatory cybersecurity culture.

In our future exploration, we will delve into crucial dimensions: learning and training, crafting the perfect incident team, leadership in crises, self-assessments, preparations, and the theory of learning after a crisis. The journey to cyber resilience demands perpetual commitment to refining processes and influencing factors.

In this challenging landscape of cyber threats, organizations must adopt a mindset of continuous improvement to stay ahead of potential crises. Let our commitment to agility, adaptability, and improvement not only withstand the challenges of today but also fortify our organizations to emerge resilient in the face of tomorrow's uncertainties.

1 https://philpapers.org/rec/AHRAIC

CYBER
CIRCLE

Cyber Circle, located in Switzerland, is a project that connects CISOs (Chief Information Security Officers) with researchers. This collaborative community meets every two months for an evening of valuable discussions and activities centered around their roles. The focus is on providing insights, facilitating cross-industry learning, enabling external peer networking, and conducting practical workshops. The ultimate goal is to establish improved cybersecurity principles, including human-centered security, within companies.

Join Cyber Circle and become part of a friendly community shaping the future of cybersecurity!

Circle hosts:
Milena Thalmann, White Rabbit Communications
Stefan von Rohr, Peer Consult
Peter Kosel, cyberunity

Based on Cyber Circle Season 3 / Session 1, Zürich, January 2024