JUMPSEC

THE SCIENCE BEHIND CYBER SECURITY SIMULATIONS

Dray Agha | Security Researcher

Daniel Green | Strategy Lead

Why simulate a cyber security crisis?

This article is the first in our series on the Science Behind Cyber Security.

Many organisations can underestimate the importance of simulating a cyber incident. But there are few things as important as your readiness to respond to a cyber incident; exciting tools are just one part of the equation and are nothing without the right people and processes to drive them. We discuss the psychology and methodology of a good crisis simulation, and the value of stress-testing your cyber security defences.

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

The importance of crisis simulations in cyber security

Cyber attacks (in particular those of the Ransomware variety) have never been more prevalent. To date, traceable ransomware payments have racked up to more than $42 million this year. All of the organisations forced to respond to these attacks were sent into crisis mode. Some will have seen the entirety of their corporate infrastructure encrypted, bringing their business operations to a grinding halt.

An organisation's readiness to respond is arguably the most important aspect of resilient cyber operations. At JUMPSEC, we have seen the impact of failing to practice and rehearse crisis management plans and procedures many times before. In an incident, being able to quickly mobilise, contain, and decisively intervene is vital to avoiding a full compromise following a breach.

This year's record numbers of vulnerabilities weaponised, attacks faced, and ransoms paid serve as a reminder of the importance of cyber readiness. This begs the questions:

- How many of the worst affected had containment and recovery plans which were untested?
- How many had prepared for a ransomware attack scenario specifically?
- And how many had no plans at all?

JUMPSEC have no doubt that those organisations with improved readiness to respond will have fared better than those without. This is because simulations are scientifically one of the best activities for your cyber security posture.

Despite this, many organisations have failed to realise the benefits of undertaking cyber crisis simulations. There are myriad reasons. For example:

- Executives may not understand the importance or value of a cyber security simulation.
- It may be difficult to find the time to bring senior decision makers together.
- There is limited understanding of the best way to run such an exercise.

However, organisations who have invested in their preparedness to respond to an incident as a business, rather than observing cyber security as 'just an IT problem' are able to significantly reduce the severity and impact of a breach.

Crisis simulations of different flavours proliferate in the cyber security marketplace. JUMPSEC's view is that the most effective simulations leverage a scientific method in both their **methodology** and **psychology**.

This article will explore why regular simulations should be a core component of your cyber security activities, and how organisations can optimise their simulations using scientifically proven methods to generate long-lasting improvements for both individuals and organisations.

The history of crisis planning

Organisations adhering to risk management best practices have formally planned for disaster and disruption since the 1970s when business continuity management first emerged as a discipline. Business continuity management was created in response to the technical and operational risks that can undermine an organisation's recovery from hazards and interruptions.

When business continuity management first emerged, organisations aligned their plans with catastrophic natural disasters – floods, fires, and earthquakes – recognising them as the most destructive unexpected and unplanned events they could face.

The goal of effective business continuity management was to maintain and/or restore operational functionality in the face of these disruptions whilst avoiding systemic disruption to the operation of the systems, facilities, and infrastructure that businesses relied on, and ensuring employee safety.

Crises can be planned for, though they may materialise in unexpected ways. **To ensure that one's plans can withstand unknown forms of crisis, they must be tested, rehearsed, exercised; simulated.**

Simulations before cyber security

Simulations as a method of contingency planning have existed for centuries. While post-war social scientists refined preparedness exercises, military strategy has relied on simulation for millennia. Training, drills, and war games have been utilised throughout history, from the ancient tactical texts of Sun Tzu to the Enlightenment-era military guidance of Clausewitz.

After World War II, these preparedness practices were developed by RAND researchers who utilised psychology and other human sciences to create simulations, geared around life-or-death situations. Still, the ultimate objective of these post-war simulations was to give the responders to a crisis greater efficiency and flexibility when in the face of an emergency.

Simulations then were designed to equip a person with the methodology and toolkit to withstand the pressures of a crisis. Today, the simulations and training of emergency responders (police, paramedics, firefighters) similarly equip them with the ability to unconsciously react without hesitation to terror attacks, burning buildings, and injured civilians.

Whilst emergencies of this calibre and severity do not occur quite the same way in cyber security (for the most part), we can still extrapolate the simulation methodology that emergency responders undergo to prepare them for unconscious yet effective responses to crises.

> **Cyber security has different needs, challenges, and objectives compared to these other contexts. But the science, reasoning, and rationale behind them are still applicable.**

Who simulates a cyber security crisis?

Unsurprisingly, military institutions are one of the prominent groups to perform cyber simulations.

For military actors, simulations are a proven strategic tool to test and enhance their cyber capabilities. For example, In November 2018, NATO organised an Estonian-based cyber simulation between seven hundred participants drawn from over thirty-two countries. The key objectives of NATO's simulation were to test strategies, policies, and procedures in cyberspace, and foster cooperation and coordination across the various institutions and individuals taking part.

Financial institutions are another key player who simulate cyber crises. Highly regulated industry sectors (such as Financial Services & Banking) are leading the way with recent consultations and upcoming legislation, including the European Commission (EC) with its Digital Operational Resilience Act (DORA) initiative and the recent consultation on operational resilience by the UK Financial Conduct Authority (FCA).

In recent years, operational resilience for organisations has become increasingly cyber-conscious. In particular, the FCA's consultation on operational resilience focuses on the definition of 'impact tolerances' for 'severe but plausible' disaster scenarios.

The setting of impact tolerances requires the organisation to determine the potential operational impact of an event, the precise timelines required to restore normal operations, the impact upon operating capacity and performance during the disruption, and the duration for which such a level of disruption is acceptable.

> **Together, these metrics provide a cohesive test and analysis of whether current contingencies lie within acceptable risk tolerance parameters, and prioritising improvement initiatives accordingly.**

The Bank of England, for example, coordinates simulated crisis exercises to gauge how resilient the market can remain, or rather how adequate contingency/incident response plans are. A key finding from one of their simulations noted that different organisations understand cyber security with their own culture and institutional language, with ranging levels of preparedness and response efficacy as a result. This reinforces the importance of testing one's own level of preparedness, and identifying specific, contextual improvements.

What is a cyber crisis simulation?

In a cyber security context, disaster recovery and incident response plans are taken from paper into practice through a simulation. Cyber simulations are designed to assess how security controls, security culture, and security operators combine to examine their effectiveness in the context of a real-world scenario.

Crisis simulations are an incident response plan brought to life, tested in the safe space of an 'experiment'. Such experiments take the form of a fictitious scenario grounded in real-life, executed in a desk-based table-top setting. Participants follow the scenario and influence the outcome by responding to injects, where they are prompted to intervene, act, and respond to the crisis as it unfolds.

What is unique to cyber simulations?

In the corporate world most simulation exercises are highly regimented. These are things like working offline to simulate the loss of digital systems or practising the response to a fire or flood. These plans are designed around scenarios that rehearse the organisation's response to the crises, laying out the optimal playbook of actions and decisions to minimise the risk. They typically follow a prescriptive set of steps in a highly controlled and detached environment. It is often clear that these exercises are performed primarily for compliance reasons first, preparedness second.

Cyber risk events, however, are highly unpredictable. It is nigh impossible to meticulously plan out a step-by-step response to a crisis with such a range in potential variables. The risk posed by cyber attack to organisations with large, dispersed operations is also much higher than an incident constrained to a specific geography or premises. **In essence, cyber attacks have the potential to be of a comparable or greater magnitude to a severe fire or flood whilst having a much higher likelihood of occurrence.**

Effective response to a cyber attack therefore requires **adaptive capabilities** which are not restrained to strict plans or specific controls. This means that an effective simulation exercise must be realistic and engaging for participants, designed to build such reflexive capabilities without following an exact process.

Let's take an example scenario, in this case, a ransomware attack. There are many variables that can influence how the incident response plays out, and therefore how the organisation should optimally respond to reduce the risk, including:

- The specific threat actor, their goals, and the tactics, techniques and procedures (TTPs) used (e.g. type of payload delivered, specific ransomware variant, attack path across the environment).
- Attacker technical goals (encryption, data exfiltration) and overall objective (ransom, data extortion).
- Method of breach, point of origin on the network, and method of malware propagation.
- Extent of compromise and systems infected / disrupted.
- Time of day the incident occurs and is detected.
- Geolocation of the incident and breached systems.

There are, of course, some broad parameters that can be and need to be prepared for. For example,

- What is the chain of command and decision making in the incident scenario?
- How will communications within the organisation be maintained?
- How will remote access to systems be facilitated to enable forensic investigation?
- Who and how will be responsible for reporting the incident to external parties such as regulatory bodies, customers, and the media?

It's clear that effective response is not about exhaustive preparation; it's about maintaining well-drilled and adaptive capabilities (across people, process and technology), which can be applied across many unpredictable scenarios.

Therefore, it is more important to regularly exercise the response to a crisis than to document the optimal response to all potential attack scenarios. In the example above, having a highly trained and well-drilled team, following pre-approved decision-making guidelines, and enabled by the tooling to quickly contain and neutralise a threat, will be far more effective in responding to a unique incident scenario than an organisation relying solely upon prescriptive playbooks or plans.

Improving simulations with science

Simulations make real the consequences of decisions. Simulations are really exercises in making the unknowns 'knowable'. By following a simulation, participants rehearse their real-life roles and learn what actions are appropriate, expected, and contextually correct. **Stepping through a 'play scenario' seems trivial, but it offers security and non-security personnel a chance to allay their anxieties in a controlled environment.**

Controlling the emotional impact when simulating a crisis

Live simulations seek to re-create the **chaotic atmosphere** of a real catastrophe. At a time of crisis, security responders are dealing with a psychological flood of different emotions. These emotions **paralyse defenders, preventing them from reclaiming control.** Experiencing these emotions for the first time in the face of an attack, without knowing what one is supposed to do next, is the primary factor which undermines an organisation's readiness to respond.

Chief among these emotions is **anxiety over the correct decisions to make when faced with the unknown. For example:**

- **(As an analyst)** Am I responding to this appropriately, or is this a false positive that will interrupt critical business operations?
- **(As an executive)** Do I know what my role is and what is required of me during an incident?
- **(As either)** Will my decision make the situation worse?

Plans and safeguards can be deployed to manage an array of technical and operational challenges, but the emotional impact of a crisis upon security operators and wider non-technical personnel is often overlooked.

Through exposure to pressure, simulations enable a responder to experience and then control the high-pressure emotions that emerge in crisis. Rehearsing 'under pressure' in the present will not wholly mitigate future pressure, but the responder is placed in a controlled experimental situation where lessons can be learned safely without real-world consequences.

The neuroscience of simulation

Neuroscience supports that the physical act of following a set procedure habituates the processes (and therefore the plan) in the muscle, brain, and nervous system. **By rehearsing a scenario, a responder's body and mind are better shaped to respond to a crisis flexibly and efficiently.**

According to Constantinidis and Klingberg, **'Working Memory' is a mechanism within the brain to recall relevant information whilst in the middle of activity.**

Training, drills, repetitive exercises, simulations - all of these have been evidenced as capable of increasing the capacity of Working Memory and thus increasing the effectiveness of completing a task.

Working Memory, and the brain overall, has impressive plasticity. The encoded memories of events, places, habits, and motor skills from one activity can be seamlessly deployed in new but vaguely similar situations. In essence, training in one situation leads to transferrable cognitive capabilities for another situation.

There is a cognitive objective to running simulations. Simulations literally create 'mental shortcuts' that allow a responder to pre-consciously recall information pertinent to a real-life crisis. Through exposure to high pressure, the brain can control the physiological stress and better process emotions, which allows for effective decision making during a real crisis.

The objective of a cyber security simulation is to foster 'Working Memory' (read 'muscle memory') by enabling responders to unconsciously recall how best to deal with a crisis. For a simulation to be effective, it should closely replicate the actual surroundings of your organisation responding to a crisis. By familiarising ourselves with surroundings during a simulation - the building, the office space and equipment - we habituate our Working Memory with the space in which we will respond to a real incident.

Taking simulations seriously

Executive management in an organisation may hesitate for a number of reasons over the decision to fund a simulation. **One possible concern is that employees may not participate seriously and treat the event as a bit of fun, as it is not a 'real' attack.**

The scientific evidence does not support this concern. There is little risk that participants will not take the event seriously by pitching the simulation with the right tone, theatrics, props, settings, and context. The facilitators can carefully cultivate the simulation atmosphere to create a serious ambience that would encourage responders to behave as if the event was real.

And even if they do, humour does not undo the cognitive progress that participants undergo throughout the simulation. Humour, even at times of genuine crisis, helps to unwind the tension of an event and foster better relations between responders who are all under stress. Creating an atmosphere that engages participants without wielding an authoritarian hand is the most conducive to improvement.

Gamification in simulation

Ludic science is a well-established field of research dedicated to understanding how various forms of 'play' can be leveraged to educate people. Consider, for example, how children learn social negotiation and creative problem-solving skills in their developmental years through play. This premise can be applied to adults: forms of play can instil transferable skills and lessons

Research has demonstrated the strength of learning cyber security practices through simulation. Games, play, simulations - all exercises with gamified mechanics - have facilitated knowledge-creation and behavioural learning. Human behaviour can be gamified and shaped by these practices. Cyber security simulations engineer a crisis, and by playing through this crisis, the participants are challenged to creatively problem solve and consider the varying impacts of their decisions in the game.

Ethical considerations

On the other hand, there is an argument that hyper-realistic exercises can harm participants through exposure to unnecessary stressors.

By replicating stressful events, there is the risk responders will internalise the ‘fictional stresses’ on a real physiological and psychological level. The organisers of a simulation should take seriously the emotional toll a simulation can have on employees, especially when stress can manifest from unexpected pressures.

One example is that lower-level employees will feel pressure to perform well, as they may not be sure if the ‘results’ from this simulation will be used against them. Another aspect of stress is that higher-level employees and employers may feel pressure to make the right calls when improvising. Their leadership may feel scrutinised by external and internal eyes. Thus, it is important to state from the outset that a simulation is not trying to catch out and admonish employees who make mistakes. Instead, a simulation is an experiment – and can be fun.

Kierkegaard was a 19th century Danish philosopher. He had a very different perspective on what anxiety was and what caused it. As sentient, thinking beings, we are conscious of the endless decisions to make, and we cannot be sure of the outcome. According to Kierkegaard, this creates anxiety, the “dizziness of freedom”, as he put it. Bringing up Kierkegaard is not a random aside, but a way of framing the emotions one may feel during a simulation. **Yes, anxiety is never a good feeling, but understanding that we feel anxious in the face of risky but important decisions is an obvious, and valuable, connection to make.** By rehearsing a response and associating the emotions we feel with the correct actions, they can guide our decisions instead of impeding them.

To ensure the ethics of a simulation, it is important that responders are given appropriate context to:

- What a simulation is, how they are being measured, and what the exercise is for.
- How to manage their feelings of anxiety and the value of simulating the exercise.

Debriefing at the end of the simulation is an important mechanism to not only gather insight for how to improve processes but is also an important mechanism to help participants to achieve catharsis and articulate their views.

A final word on cyber simulations

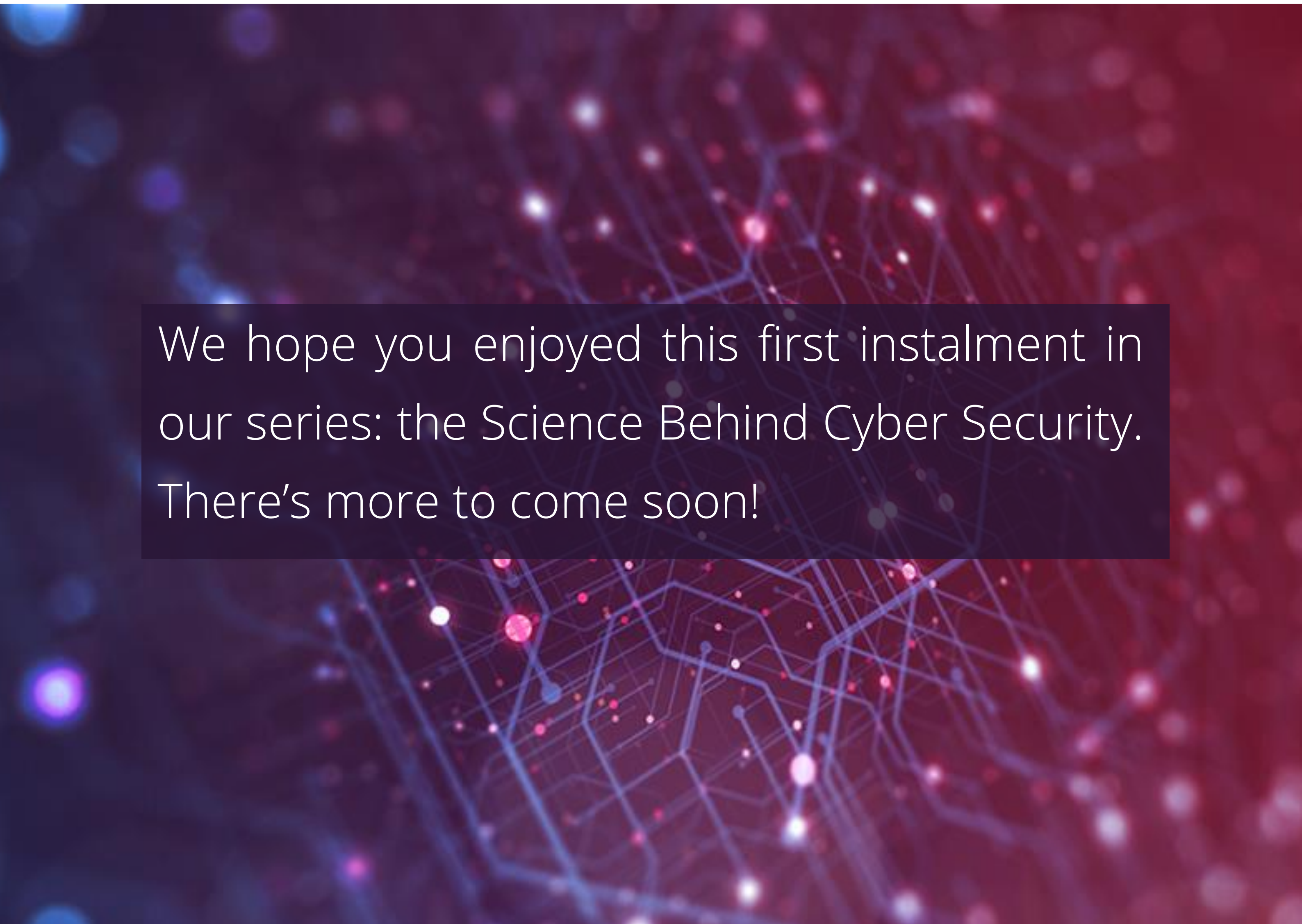
Simulations are a proven method with neurological-cognitive benefits, and an organisation can use them to assess and refine their resilience. But simulations must reflect the real world. This means that a simulation must be led by realistic scenarios that represent the reality. This means considering networks that are not effectively segmented, that contain legacy machines that remain unpatched, or security controls that were not rolled out due to the potential impact on business performance overriding the perceived security risk.

The best simulations are informed by technical exercises to provide a realistic context, making sure that your crisis management teams are given the information and tools they would have in the real world. This may make the scenario challenging to respond to (as is the case for most victims of cyber attack), but most accurately reflects reality, and provides the greatest stimulus and opportunity for improvement. Participants must be both enabled and authentically constrained by their surroundings to identify gaps and uncover limitations, leaving the organisation better prepared to respond in a real-world scenario.

There's a great aphorism relevant to simulations that helps with framing this kind of real-world scenario:

"The knight in shining armour is a knight who has never had his metal truly tested".

In essence: it's acceptable to come out battered and bruised from a simulation if it enables you to harden the weak points in your armour before they are exposed in real combat.



We hope you enjoyed this first instalment in our series: the Science Behind Cyber Security. There's more to come soon!