People inspired cyber resilience

Part 1 of 2

February 2021

Murray Pearce, Director, Bright Cyber

EXECUTIVE SUMMARY

Bright Cyber is a Cyber Resilience Solution Provider with specialist security assurance. These include ISO 27001, privacy consultancy, GDPR advice and technical expertise.

We put people at the heart of cyber security by focusing on four levers which are as follows: 1. Human cyber resilience 2. Breach prevention and detection 3. Incident response 4. Automation and security management. Used together these will help customers improve their cyber resilience.

In part 1 of this whitepaper, we advocate the view that people, who are working as part of a high performing team, are the single most important resource an organisation can leverage for creating cyber resilience.

Readers will learn why we believe that people should be at the heart of cyber security strategy, how to maximize the impact of their people by building a high performing team, and where people sit in the journey towards building a cyber resilient organisation.

In part 2, we will explore our "4 Levers of Cyber Resilience" and how these can be applied as a journey to help organisations succeed in experiencing fewer cyber security incidents. This will result in lower cost per incident, allow organisations to recover faster, and also allow for scale in meeting the challenges which are present in a world of digital transformation.

Our intent and overall outcome of this whitepaper is to give you new insights, pathways and actions to consider which will supplement your cyber security best practice.

INTRODUCTION

What do we mean by cyber resilience?

> Cyber resilience is the ability for organisations to operate effectively during cyber adverse conditions, such as cyber incidents and periods of increased risk, ranging in anything from a crisis or digital transformation, for example.
>
> It involves being prepared to prevent, detect, correct, and recover from cyber incidents.

The importance of cyber resilience

> Organisations are innovating at a never-before-seen pace as executives seek to remain competitive, pursue new opportunities and make improvements through digital transformation.
>
> New business models, working practices and technology, such as remote working and cloud adoption, are being implemented with significant benefits but, whilst these may bring improvements to today's way of doing business, they also bring increased cyber security risk with them.

"Digital transformation (DX) is at the centre of modern organizational strategies. IDC estimates the economic value of DX at over $20 trillion, or over 20% of global GDP, with direct investment of over $8.2 trillion as organizations and entire industries transform themselves to compete in the digital economy." Source: IDC 2021

The full impact of digital transformation on cyber resilience is often overlooked. Cyber security teams, already struggling with a complex threat landscape, are becoming increasingly overwhelmed and less able to react. In addition, employees are becoming confused about how they should work securely.

Building cyber resilience is critical in this challenging environment to prevent organisations from losing control and becoming vulnerable to bad actors, who are actively seeking to exploit them, and from employee misadventure, all of which results in cyber security teams being less able to respond when incidents do occur, which inevitably they will.

High cyber resilience is a key success factor for organisations in progressing business goals without being impeded, protecting operational capability and maximising opportunity. Performed properly, cyber resilience moves cyber security into a new paradigm as a business accelerator.

Covered in this whitepaper:

Part 1

- Why people first?
- How to build a high performing cyber resilience team
- Impact of a high performing cyber security Team

Part 2

- People in the cyber resilience journey
- 4 levers of cyber resilience
- Best practice adoption

Benefits of reading this whitepaper:

- Actionable insights that will strengthen your first line of defence; people.
- Straightforward advice on how to increase cyber resilience.
- A customer journey that will help you experience fewer cyber security incidents, with reduced cost per incident and faster recovery.

Why people first?

As stated in the UK National Cyber Security Centre’s Security Toolkit for boards, organisations should "put people at the heart of security” Source: NCSC 2019. This is certainly the right approach!

People possess the best computer system ever invented - the brain!

People are more intuitive, agile and powerful than any single system. Human beings are better able to identify new problems that technology might miss, adapt to change, respond to incidents in real-time and solve complex problems.

Whilst people have weaknesses, and technology has an important role to play, we should never forget that people are still the single most powerful resource available to organisations, especially when working as part of a high performing team.

How to build a high performing cyber resilience team.

Who is in the team?

From a cyber resilience perspective, the team should be as diverse as possible. Executive leaders, management and all employees as well as any relevant external people in your trusted network, your eco-system of vendors and trusted partners, such as Bright Cyber, should make up the team.

The five characteristics of a high performing team

Through the *Five Dysfunctions of a team framework*, we see that high performing teams can be distilled into five characteristics. These are *triple purpose, trust, mutual accountability, positive conflict and mental fitness*. This concept is inspired by the work of Patrick Lencioni in his work *The Five Dysfunctions of a Team* and Shirzad Charmin's work *Positive Intelligence*. Both Lencioni and Charmin are respected world leaders in coaching and leadership.

Triple Purpose

High performing teams must be aligned to a common vision and with goals that relate to, firstly, individuals in their roles, secondly, the actualisation of their teams and, lastly, through support from the organisation.

It starts with the leaders! Cyber leaders must be welcomed into all areas of organisational strategy, without silos, and they must come prepared to help their fellow executive leaders by understanding and advising on relevant risks, asking the right questions and, importantly, acting as a facilitator in achieving business outcomes.

It is in the balancing of business outcomes with acceptable risk, specific and real to the organisation, that leaders will find and agree on a shared vision and goals for cyber resilience.

This is all achievable, in spite of the challenges it poses.

Trust

High performing teams thrive when there is trust. It is difficult to get momentum without trust, and breaking trust will be destructive, slowing the team down, potentially bringing it to a standstill.

Executive leaders must lead by example by advocating, and living, the shared responsibility of protecting the organisation. Leaders must nurture a culture that values cyber resilience and the attitude that everyone has a part to play.

They should consider how to link cyber resilience to business outcomes as they would with any other essential function, such as marketing and finance, and communicate this as part of the strategy so that it connects cyber strategy to the success of the organisation, their employees and desired outcomes.

People should be encouraged to raise questions, issues, and concerns.

To err is human, and so leaders must foster a team culture where employees know that they can highlight mistakes to internal security teams without fear of reprisal for accidents and that in doing so they are helping the organisation.

Trusted partners need open and honest communication too, under an NDA if necessary, so that they understand the business and can advise effectively by bringing their experience and capabilities to help you achieve your mission.

Establishing this "trust without borders" mentality will help break down the silos that often plague cyber security and increase risk.

Mutual accountability

One of the most persistent complaints heard generally from cyber security professionals is that there is a lack of support and shared responsibility, especially when things do go wrong. This has resulted in high cyber security employee turnover, burnout, depression and addiction Source: Forbes 2019.

In a recent McKinsey podcast "Boards and Cyber Security" , broadcast in February 2021, John Noble**,** former director of the United Kingdom's National Cyber Security Centre, expressed his concern in this way:

"Cyber security is an issue for the whole organization. Whether it is in advance of or during an incident, you should not just leave it to the chief information officer and the technical team. Leaders need to decide how to manage the tensions between usability, security, and cost, and that is very much where we need the board challenging and testing processes." Source: NCSC 2021

Similarly, executive leaders can express frustration when cyber resilience programs interfere with achieving business outcomes; they want a business-first mentality from cyber security leaders. Understanding it is not possible to perfectly protect an organisation, cyber security leaders need to help their organisation's progress by sharing this understanding and encouraging a realistic view.

In addition, organisations too often feel that partners and vendors are only interested in selling a point solution and not in helping them improve their organisation's cyber resilience over the long term.

We recommend that there are appropriate, documented expectations in place, whether for executive leaders, cyber leaders, employees or external parties, which are tied to performance measurements to ensure mutual accountability.

Positive conflict

In order to achieve the benefits available from digital transformation, organisations are undergoing rapid innovation.

Cyber security leaders must adopt a similar innovation mind set when building cyber resilience strategy by actively incubating new ideas, assessing new technology, challenging existing practices and "perceived" wisdom, and seeking improvements in a safe and constructive environment.

This process increases the ability of the team to scale and adapt to new challenges and threats.

Mental Fitness

Companies are becoming increasingly aware of the benefits of looking after their employee's mental health. This is a good start as it can help employees feel less stressed or overwhelmed and reduce absence or loss of employee.

However, we recommend companies look beyond simply managing stress and move towards building mental fitness, as this will ensure individuals, teams and organisations are operating at their peak potential performance more often.

Impact of a high performing team on cyber resilience

High performing teams with trust and cohesion enable their organisations to be more successful in achieving their business outcomes, as they bring enhanced capabilities.

- 19% better diagnosis

- 30% higher productivity,
- 3x creative problem solving
- + employee morale and happiness

Source: Positive Intelligence

These qualities translate directly into cyber resilience efficacy by improving the risk position, alleviating resource constraints, faster diagnosis and resolution of incidents, meeting digital transformation challenges and improving staff retention.

Summary

Cyber resilience is a team sport and comes from a team with a clear understanding of its goals (purpose), open communication (trust), a deep sense of shared responsibility (mutual accountability) and willingness to challenge in order to improve (positive conflict). This will result in a high performing team, helping the organisation experience fewer incidents and making it better able to respond them when it does.

Can we help you?

If you would like further information or to discuss how we can help you, please email murray.pearce@bright-cyber.co.uk

About us

Bright Cyber are a Cyber Resilience Solution Provider and ISO 27001 experts. We put people at the heart of cyber security and focus on 4 levers: people, technology, response and automation to increase cyber resilience. We help organisations experience fewer incidents, with a lower cost per incident and a faster recovery.

References

All webpages used in this whitepaper were accessed in February 2021.

IDC
Worldwide Digital Transformation Strategies (idc.com)

McKinsey
https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/boards-and-cybersecurity

NCSC
https://www.ncsc.gov.uk/collection/board-toolkit/growing-cyber-security-expertise

Patrick Lencioni's
The Five Dysfunctions of a Team

Shirzad Charmin
Positive Intelligence

People inspired cyber resilience

Part 2 of 2

February 2021

Murray Pearce, Director, Bright Cyber

Part 2: People inspired cyber resilience

The second part of this whitepaper focuses on people as the first of four levers in building cyber resilience. The themes we address are:

- People on the cyber resilience journey
- 4 levers for building cyber resilience
- Adopting best practice

People in the cyber resilience journey

In Gartner's eBook "Rethink the Security & Risk Strategy", accessed February 2021, distinguished VP analyst, Tom Scholtz, muses that it is time for CISOs to re-invent security and lays out 6 principles for building trust and cyber resilience. They should:

- Shift to risk-based decision making and away from checkbox compliance
- Begin supporting business outcomes rather than solely protecting infrastructure
- Become a facilitator, not a defender
- Determine how information flows; don't try to control it
- Become people-centric and accept the limits of technology
- Invest in detection and response, and stop trying to perfectly protect the organisation

These principles are predominantly about people, mindset and behaviour.

Therefore, the first lever in our cyber resilience journey is to focus on *human cyber resilience*, a combination of people and process, before moving onto the next phase which is *breach prevention and detection*, which has a high technology focus and, thirdly *incident response*, a process for when things do go wrong and then finally, *automation and management* to help organisations scale.

These four levers of cyber resilience can be used as a tool to improve cyber resilience significantly, creating a clear roadmap which will enable organisations to meet the aspiration of the 6 principles above, moving cyber security people towards the role of "business accelerators".

Ultimately, this means organisations experiencing fewer cyber incidents, with less cost per incident, and a faster recovery, so that they can get on with business.

The 4 levers of cyber resilience

Human cyber resilience

Human error is a leading cause of breaches – after over 20 years in the information security industry we can attest to this. The use of technology alone, as a cure for human error, will not prevent cyber incidents.

We believe that your people are your first line of defence and, like any good army, they need leadership, tools and training.

Our human cyber resilience approach has 3 components:

1. Your people

   Enhancing people inside your organisation; executive engagement, developing cyber leaders and skills, building an advanced human firewall, and cyber team "mental fitness".

2. Your network

   Augmenting your capability with trusted people outside of your organisation, including trusted advisors, solution partners, service providers, vendors, peers to augment your team so that you can fill any internal skill gaps or add resource, using Bright Cyber, for example.

3. Your planning

   Getting your people organised with strategic goals and work practices through *policy, process and technology*.

   We start by checking that your baseline cyber security is robust and then identify regulatory obligations, information flows, critical assets and the risks associated with those critical assets. Frameworks can be a useful tool to help in refining controls and technology can be added to better secure your organisation.

Breach prevention and detection

There is a wave of innovative technology that can help prevent and detect breaches, so much so that one of the pitfalls to building cyber resilience is overplaying the role of technology. Also, the marketing and sales claims of technology vendors should be carefully scrutinised.

That said, breach prevention and detection technologies are critical tools for cyber resilience, especially when you consider that the average time to identify a breach in 2020 was 207 days Source: IBM 2020.

To navigate the myriad of options, we recommend cyber security teams invest time in understanding the threat landscape and how it applies in their business, before considering whether they have the right technology or not.

Trusted partners can be very helpful too, acting as your eyes and ears in the market, highlighting and explaining new threats and the technology that can be used to address them, without a point solution focus or vendor sales pressure.

The key is to work with partners that commit to help build your long-term cyber resilience. This is the reason why we recommend treating trusted partners as part of your high performing cyber team, establishing purpose, trust, mutual accountability and positive conflict.

Incident response

More than 77% of organisations do not have an incident response plan Source: Cybint 2020. As we mentioned previously, it is not possible to protect your organisation perfectly, so planning on how to respond to unexpected circumstances should be a priority.

"Thirty-seven percent of UK companies have reported a data breach incident to the Information Commissioner's Office (ICO) in the past 12 months" Source: CSO online 2020.

We strongly recommend building a capability to respond to a major incident. This starts by accepting that incidents will occur!

We encourage leaders to be mindful of considering incident response as a capability rather than a plan, and that this capability could be activated at any time, possibly sooner than you might expect.

Your incident response capability must be simple and practical, able to be executed under pressure and defend against attacks and data breaches.

Best practices include keeping the plan to the point, without unnecessary text, starting with a checklist of *Dos and Don'ts* and making sure your cyber incident response team (CIRT) are available. All stakeholders should be identified such as business line, technical support and external parties. Critical systems' details and their associated owners are listed, playbooks and communication flows are easy to find and clear to follow.

Remember to include third party and external resources in your documentation, especially if they are supplying critical response services and capability.

There are several good incident response handling methodologies and online resources, including the NIST computer security handling guide, which we can recommend.

Automation and management

In many ways, automation and security management is the perfect bookend to human cyber resilience because it helps organisations scale and support people by removing repetitive or manual tasks, so that people can focus on solving more complex issues.

Automation, in its simplest form, deals purely with automating manual tasks which are low risk and high priority.

Automation, including smart AI technology, is becoming a critical lever for organisations as the task of maintaining cyber resilience becomes overwhelming, with a new attack every launched every 39 seconds, Source: Maryland University, and too many systems to update, alerts to respond to and regulatory obligations to meet.

Since the Covid-19 pandemic began, the FBI reported a 300% increase in reported cybercrimes Source: MC Grupo. Illustrating the added pressure that teams face today.

Once organisations are confident they have the baseline covered and critical assets protected, they should identify tasks that are time-consuming and repetitive and look at how technology might be used to automate part or all of the process. This will not only help organisations scale, but it alleviates the potential for human error.

AI is developing technology and organisations would do well to read the NCSC guidance on smart tools.

The author's own view is that black box AI, which represents most AI solutions, is open to bias and can introduce risk. Further, insights and actions taken using Blackbox AI raise many questions around accountability and therefore should be used with caution.

A more advanced form of AI, known as Explainable AI, provides transparency around how an AI tool arrives at an insight or decision. We believe this will be the future for AI in cyber security.

Lastly, and since security does not stand still, organisations need to think about how to manage their security going forward. Starting with an identified baseline, a management system will then help an organisation measure where they are in their security posture so they can make appropriate investments over time and remain cyber resilient.

Certifications such as ISO 27001 and similar frameworks may require significant documentation to maintain, depending on the context of your organisation. The documentation requirements must be updated regularly to be useful in treating risk, beyond ticking a compliance box. There is always a possibility that an organisation may implement an overly-documented system which is not practicable to maintain. This may prohibit the system from protecting information assets effectively as a result.

We recommend looking at platforms that help to automate this process. Whilst in the past these platform solutions have been very expensive, and hard to implement, today there are cost-effective and easy-to-use platforms available.

Best practice adoption

The following section has been written by Doug Drummond, Director and Co-founder Bright Cyber.

Today's enterprises increasingly utilise comprehensive software packages to improve employee performance and productivity by integrating business processes and data across the organisation. Unfortunately, for many enterprises, deploying these complex software packages is a significant challenge that quickly becomes unmanageable. Bright Cyber recommends that enterprises use the following guidelines when selecting partner deployment services for their IT environments:

1. Consider utilizing an external provider to deploy enterprise software packages

While many IT departments consider internal deployments to be the least expensive solution, complex software deployments can very quickly lead to delayed schedules and unanticipated cost overruns. An external provider that has extensive experience with the selected software can plan and deploy the solution while utilizing best practices learned from other implementations, especially when configuring software around existing business processes. Also, external deployment providers can diagnose and resolve critical issues quickly and effectively, leading to smoother implementations that stay on schedule and within budget — and often cost less over the life of the project.

2. Look for deployment providers with programs and processes that reduce deployment risk

Software implementations typically require planned downtime, and any unforeseen issues can lead to unplanned outages that affect everyday operations. Software deployment providers with established deployment processes and well-defined implementation methodologies can help minimise the potential for schedule disruptions and cost overruns.

3. Ask deployment providers to illustrate success with implementation practices that accelerate the move into production, above traditional software deployments

Faster adoption can mean a more immediate impact on business results and can often translate into a quicker return on your investment in the selected technology. Also, phased deployments can be helpful for enterprises considering large software deployments. Starting to use the software as it becomes available can allow the organisation to learn the software quickly, which means a faster payback period for the project.

Can we help you?

If you would like further information, please call 0345 257 0071 or email resilience@bright-cyber.co.uk

About us

Bright Cyber are a Cyber Resilience Solution Provider and ISO 27001 experts. We put people at the heart of cyber security and focus on 4 levers: people, technology, response and automation to increase cyber resilience. We help organisations experience fewer incidents, with a lower cost per incident and a faster recovery.

References

All webpages used in this whitepaper were accessed in February 2021.

Capita / IBM
Cost of a Data Breach Report 2020

Cybint
15 Alarming Cyber Security Facts and Stats | Cybint (cybintsolutions.com)

Gartner
"Rethink the Security & Risk Strategy"

IMC Grupo
COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes - IMC Grupo

NCSC
https://www.ncsc.gov.uk/collection/board-toolkit/growing-cyber-security-expertise
https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

NIST
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final