CYBER INCIDENT SIMULATION EXERCISES

THE TRUST BRIDGE

THETRUSTBRIDGE.CO.UK

Cyber Simulation Exercise

What is it ?

Why do one?

A Cyber Simulation exercise is a training exercise that replicates a real cyber / security / ransomware incident, and demonstrates what can happen, so you can see what to do

Prepare

Simulation gives real life, real time training for your team so they know what to expect when under attack:

What to do

When

Who to tell

Mitigate

Helps teams to understand what the risks as they carry out their daily work

Recover

If the worse happens, you learn how to recover, what are the priorities and consequences – and what not to do

The business case for conducting a cyber incident simulation

- In the third quarter of 2022, global cyber attacks rose by 28% (source: Check Point)
- over 1,130 weekly attacks per organization worldwide

- hackers are targeting sensitive consumer data
- hackers becoming more skilled at exploiting vulnerabilities.

Under the The Cyber Incident Reporting for Critical Infrastructure Act in the USA, incidents must be reported to the CISA.

- Organisations required to report a cyber incident within 72 hours to the CISA. Payment of any ransom must be reported within 24 hours of the payment

If you’re doing business within the EU, under GDPR testing is mandatory.

- Organisations need to show that they have ‘a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.’

The World Economic Forum has said that ‘fire drills’ are key for cybersecurity in all jursidictions

- Experts stress that preparing companies as a whole for cyber attacks is a key component of cybersecurity. This includes not only top executives and IT departments, but employees across an organization.

Regularly holding proper immersive simulations can help reduce cyber insurance premiums

- Cyber insurance policies are becoming far more conditional – many now either require you to conduct tests or offer discounts on insurance premiums if you do so – often meaning that the tests in effect pay for themselves

If or when things go wrong regulators will ask why you did not run simulation exercises

- The best defence for regulation or litigation will be the ability to show that you took responsible steps to be prepared

thetrust bridge™

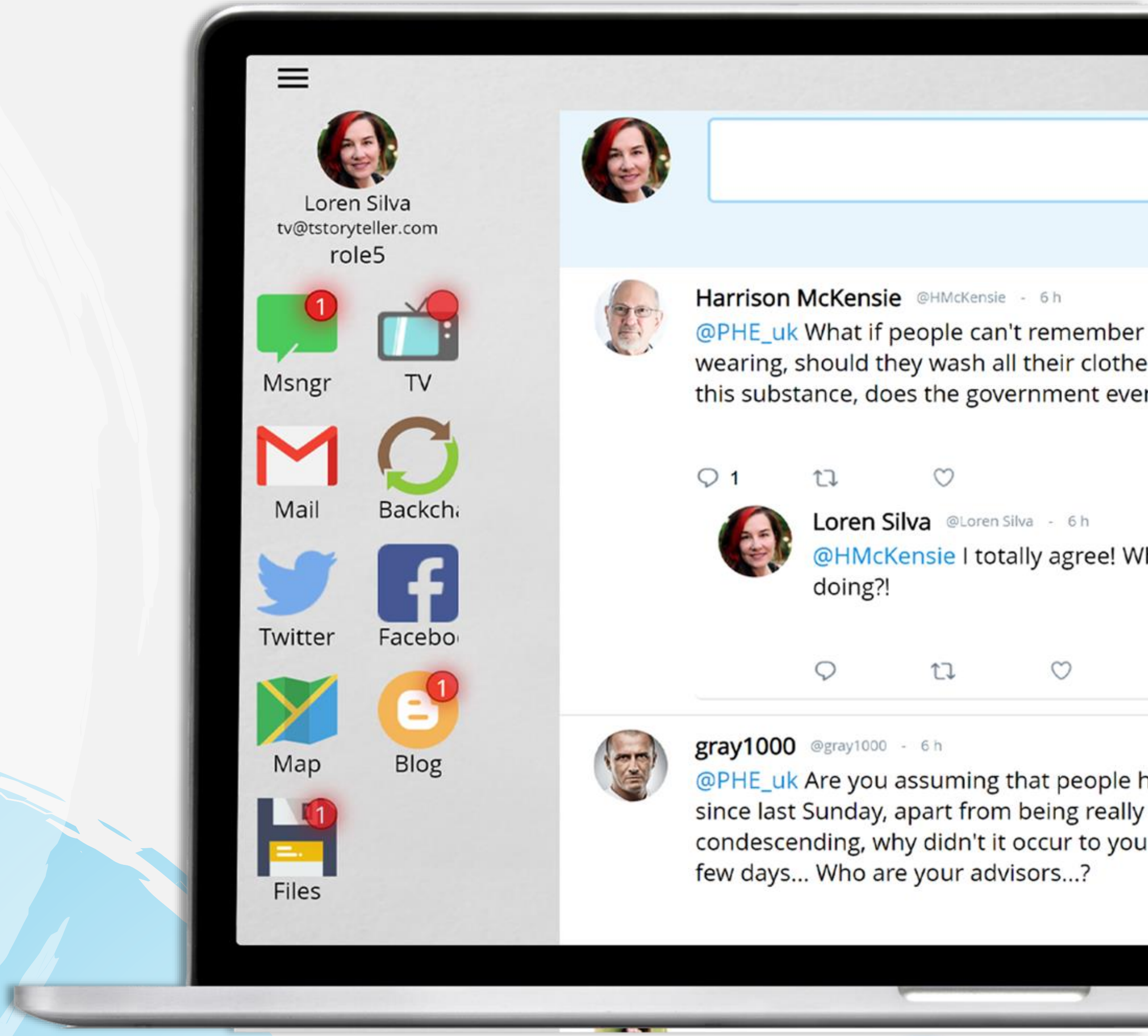
If you’re doing business within the EU, under GDPR testing is mandatory

The Crisis Team

The case for running realistic, immersive simulation exercises that really put teams to the test

Crisis exercise classes using PowerPoint won't prepare you for real-world conditions.

You need to conduct regular crisis management drills using fully immersive scenario simulations in order to properly prepare your team and ensure that they are really crisis prepared.



Loren Silva
tv@tstoryteller.com
role5

Harrison McKensie @HMcKensie · 6 h
@PHE_uk What if people can't remember wearing, should they wash all their clothe this substance, does the government ever

Loren Silva @Loren Silva · 6 h
@HMcKensie I totally agree! W doing?!

gray1000 @gray1000 · 6 h
@PHE_uk Are you assuming that people h since last Sunday, apart from being really condescending, why didn't it occur to you few days... Who are your advisors...?

Our simulation exercises include a range of media and channels to accurately simulate a real incident

thetrust bridge

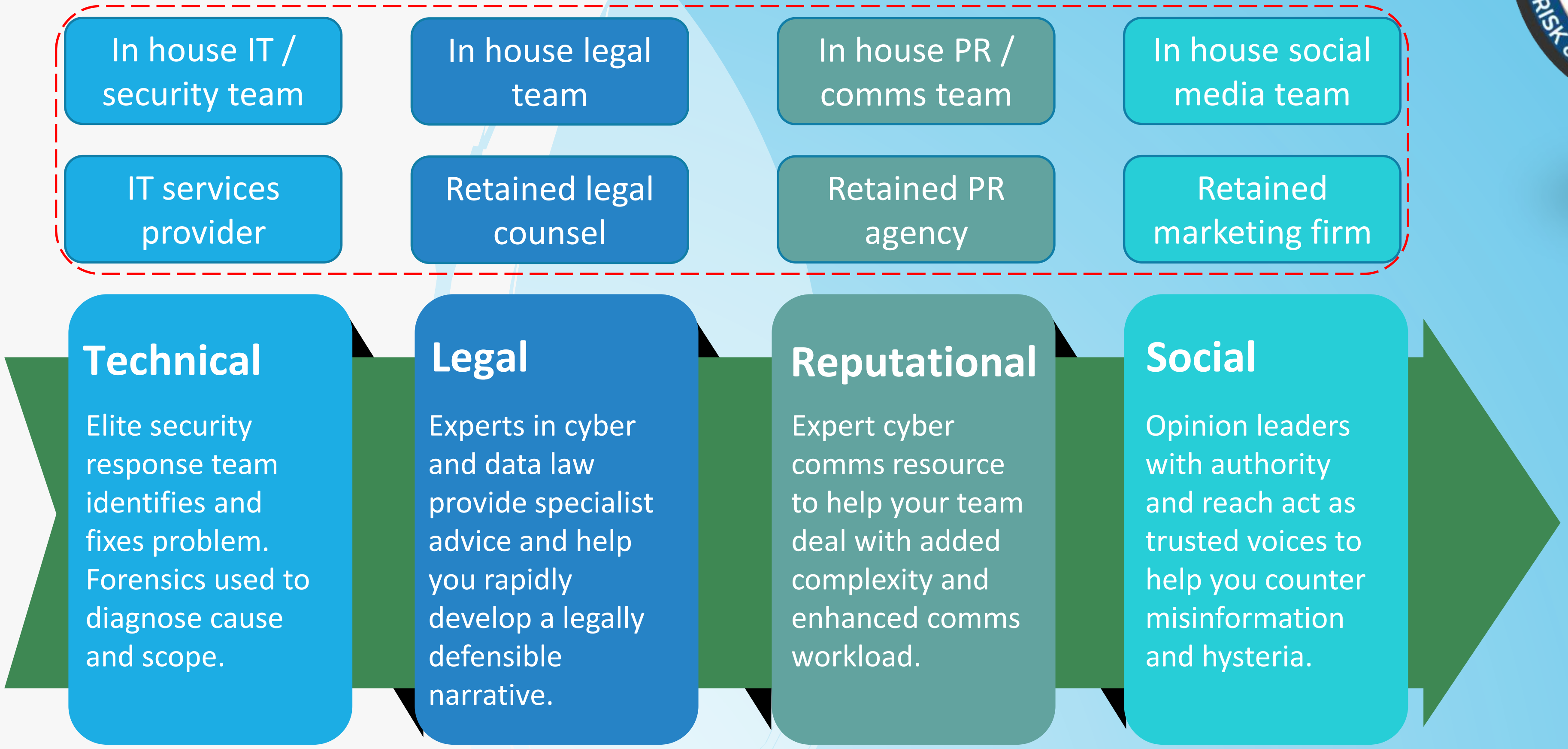
Cyber Simulation backed by the International Association of Risk and Crisis Communication

non-profit organisation that promotes research, knowledge exchange and professional development in Risk and Crisis Communication worldwide with a focus on risk awareness, crisis preparedness and incident response.

IARCC.org

IARCC's recommended approach to cyber incident response

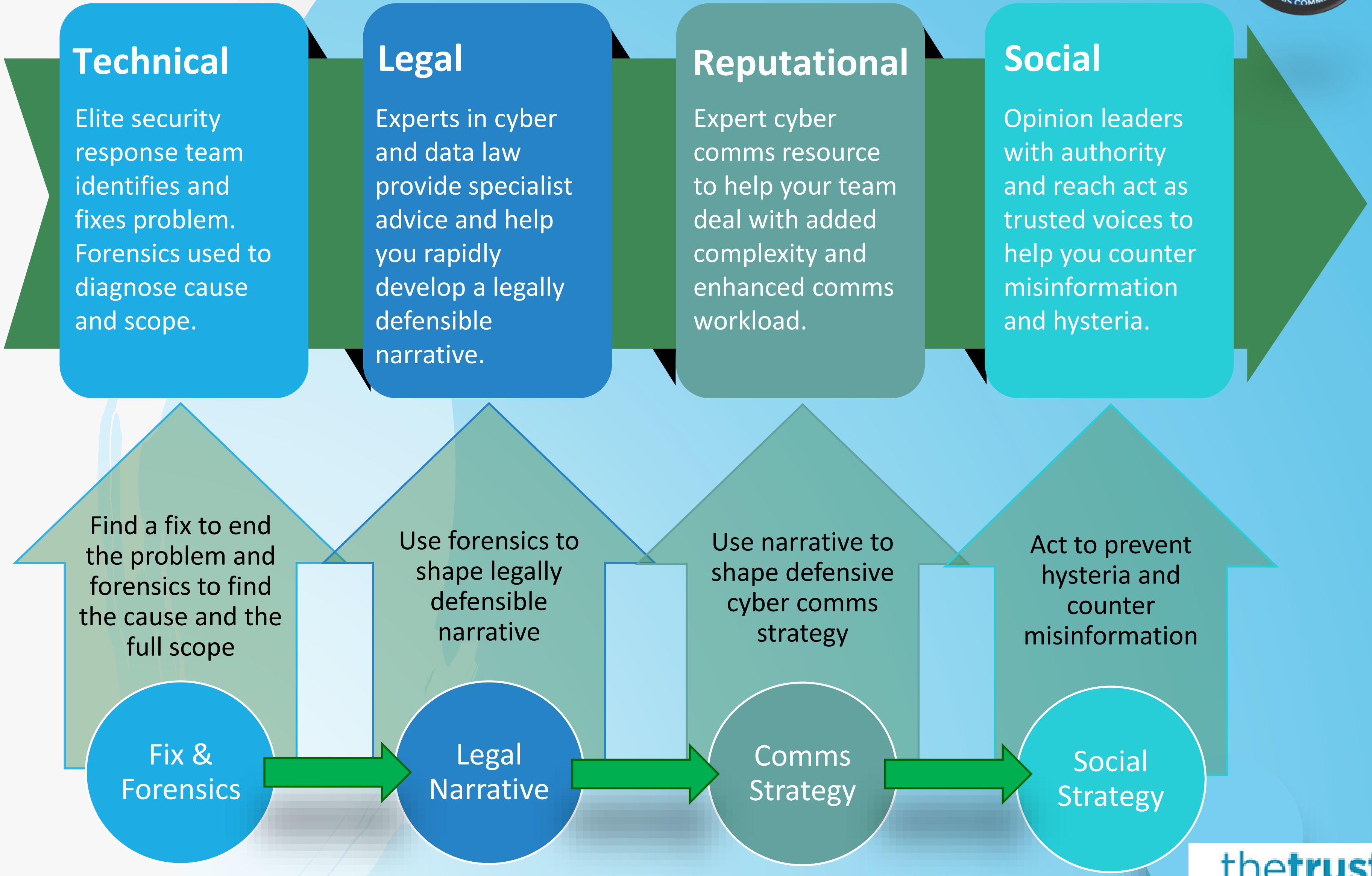
Working with Clients AND their Extended Teams



	Technical	Legal	Reputational	Social
The staff, capability and skills that you have	In house IT / security team IT services provider	In house legal team Retained legal counsel	In house PR / comms team Retained PR agency	In house social media team Retained marketing firm
The extra expert staff, capability and skills that you need in a cyber crisis	Elite security response team identifies and fixes problem. Forensics used to diagnose cause and scope.	Experts in cyber and data law provide specialist advice and help you rapidly develop a legally defensible narrative.	Expert cyber comms resource to help your team deal with added complexity and enhanced comms workload.	Opinion leaders with authority and reach act as trusted voices to help you counter misinformation and hysteria.

In a Cyber Crisis

1) You're likely to be on the back foot
2) Cyber incidents aren't instantaneous
3) You're going to get the blame



Technical

Elite security response team identifies and fixes problem. Forensics used to diagnose cause and scope.

Legal

Experts in cyber and data law provide specialist advice and help you rapidly develop a legally defensible narrative.

Reputational

Expert cyber comms resource to help your team deal with added complexity and enhanced comms workload.

Social

Opinion leaders with authority and reach act as trusted voices to help you counter misinformation and hysteria.

Find a fix to end the problem and forensics to find the cause and the full scope

Use forensics to shape legally defensible narrative

Use narrative to shape defensive cyber comms strategy

Act to prevent hysteria and counter misinformation

Fix & Forensics → Legal Narrative → Comms Strategy → Social Strategy

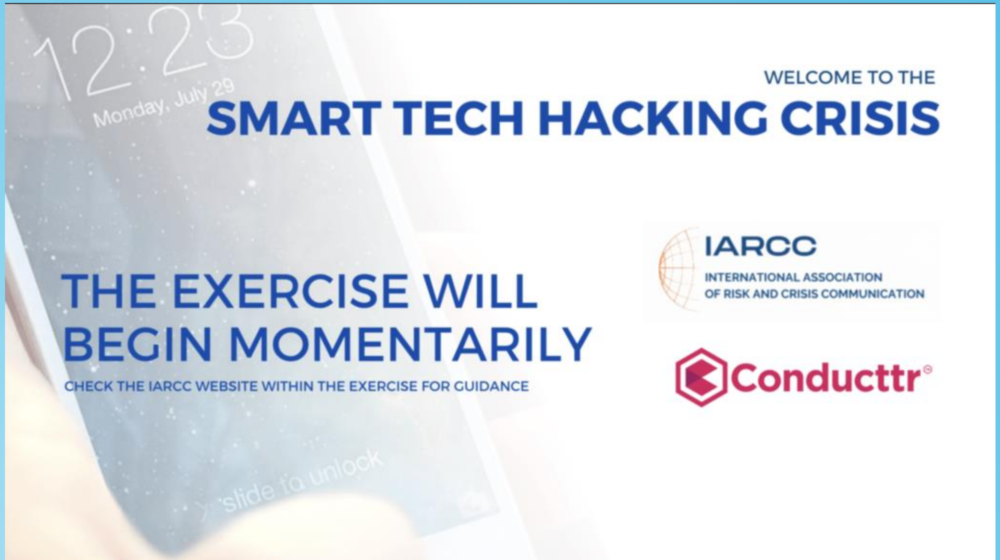
Creating Simulations for Your Organization

thetrust bridge™

Working with you

We create a bespoke simulation for your organization

The cyber incident simulation, accredited by IARCC, will give you a feel for the immersive nature of the platform



WELCOME TO THE

SMART TECH HACKING CRISIS

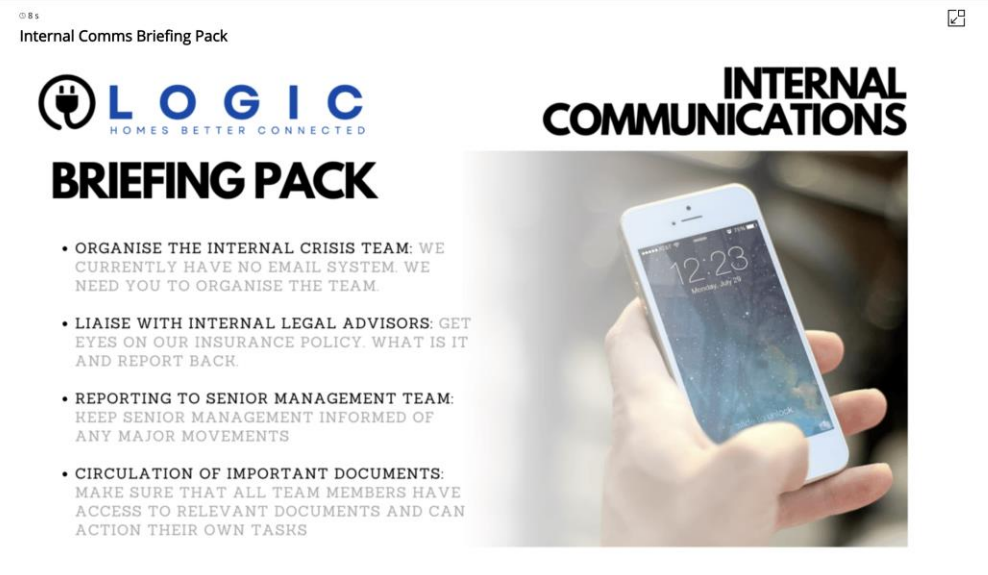
THE EXERCISE WILL BEGIN MOMENTARILY

CHECK THE IARCC WEBSITE WITHIN THE EXERCISE FOR GUIDANCE

IARCC

INTERNATIONAL ASSOCIATION OF RISK AND CRISIS COMMUNICATION

Conducttr®



8 s

Internal Comms Briefing Pack

LOGIC

HOMES BETTER CONNECTED

BRIEFING PACK

INTERNAL COMMUNICATIONS

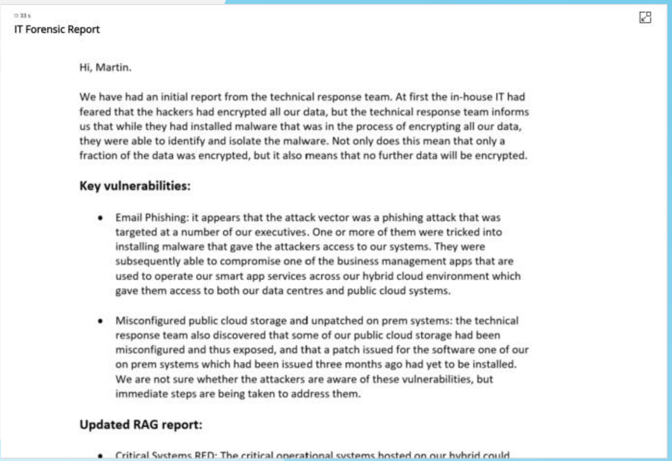
- ORGANISE THE INTERNAL CRISIS TEAM: WE CURRENTLY HAVE NO EMAIL SYSTEM. WE NEED YOU TO ORGANISE THE TEAM.
- LIAISE WITH INTERNAL LEGAL ADVISORS: GET EYES ON OUR INSURANCE POLICY. WHAT IS IT AND REPORT BACK.
- REPORTING TO SENIOR MANAGEMENT TEAM: KEEP SENIOR MANAGEMENT INFORMED OF ANY MAJOR MOVEMENTS
- CIRCULATION OF IMPORTANT DOCUMENTS: MAKE SURE THAT ALL TEAM MEMBERS HAVE ACCESS TO RELEVANT DOCUMENTS AND CAN ACTION THEIR OWN TASKS

thetrust bridge™

Working with you

We can work with you to brainstorm a flexible scenario that suits your environment

We can then develop materials for use in the simulation, including using our studio facilities to create realistic video news reports



IT Forensic Report

Hi, Martin.

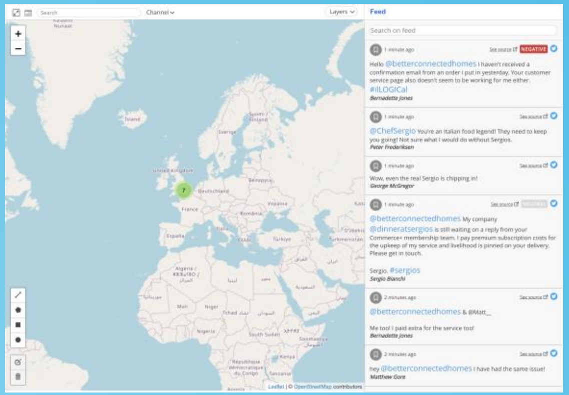
We have had an initial report from the technical response team. At first the in-house IT had feared that the hackers had encrypted all our data, but the technical response team informs us that while they had installed malware that was in the process of encrypting all our data, they were able to identify and isolate the malware. Not only does this mean that only a fraction of the data was encrypted, but it also means that no further data will be encrypted.

Key vulnerabilities:

- Email Phishing: it appears that the attack vector was a phishing attack that was targeted at a number of our executives. One or more of them were tricked into installing malware that gave the attackers access to our systems. They were subsequently able to compromise one of the business management apps that are used to operate our smart app services across our hybrid cloud environment which gave them access to both our data centres and public cloud systems.
- Misconfigured public cloud storage and unpatched on prem systems: the technical response team also discovered that some of our public cloud storage had been misconfigured and thus exposed, and that a patch issued for the software one of our on prem systems which had been issued three months ago had yet to be installed. We are not sure whether the attackers are aware of these vulnerabilities, but immediate steps are being taken to address them.

Updated RAG report:

- Critical Systems RED: The critical operational systems hosted on our hybrid could



1 minute ago · See source · NEGATIVE

Hello @betterconnectedhomes I haven't received a confirmation email from an order I put in yesterday. Your customer service page also doesn't seem to be working for me either. #iLOGICal

Bernadette Jones

1 minute ago · See source

@ChefSergio You're an Italian food legend! They need to keep you going! Not sure what I would do without Sergios.

Peter Frederiksen

1 minute ago · See source

Wow, even the real Sergio is chipping in!

George McGregor

1 minute ago · See source

@betterconnectedhomes My company @dinneratsergios is still waiting on a reply from your Commerce+ membership team. I pay premium subscription costs for the upkeep of my service and livelihood is pinned on your delivery. Please get in touch.

Sergio. #sergios

Sergio Bianchi

2 minutes ago · See source

@betterconnectedhomes & @Matt_

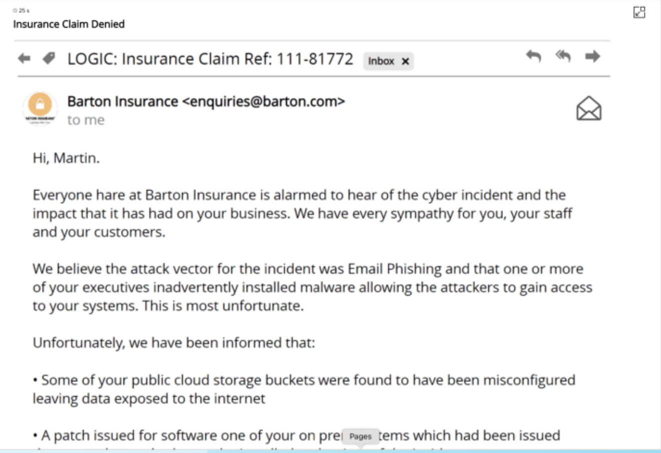
Me too! I paid extra for the service too!

Bernadette Jones

2 minutes ago · See source

hey @betterconnectedhomes I have had the same issue!

Matthew Gore



Insurance Claim Denied

LOGIC: Insurance Claim Ref: 111-81772

Barton Insurance <enquiries@barton.com>
to me

Hi, Martin.

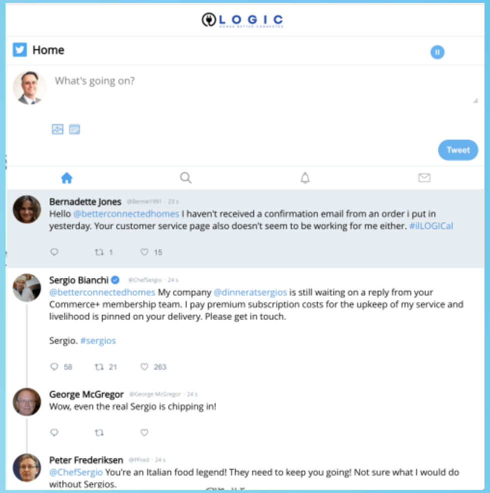
Everyone hare at Barton Insurance is alarmed to hear of the cyber incident and the impact that it has had on your business. We have every sympathy for you, your staff and your customers.

We believe the attack vector for the incident was Email Phishing and that one or more of your executives inadvertently installed malware allowing the attackers to gain access to your systems. This is most unfortunate.

Unfortunately, we have been informed that:

• Some of your public cloud storage buckets were found to have been misconfigured leaving data exposed to the internet

• A patch issued for software one of your on pre tems which had been issued



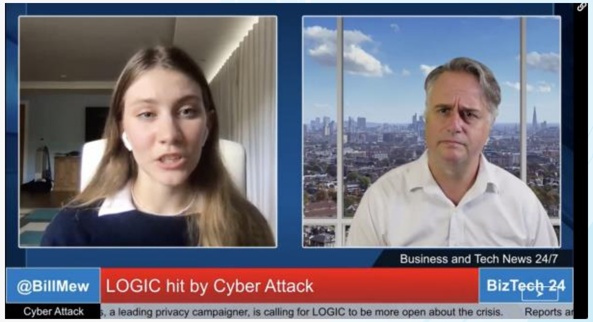
Bernadette Jones @Bernie1991 · 23 s
Hello @betterconnectedhomes I haven't received a confirmation email from an order i put in yesterday. Your customer service page also doesn't seem to be working for me either. #iLOGICal
1 · 15

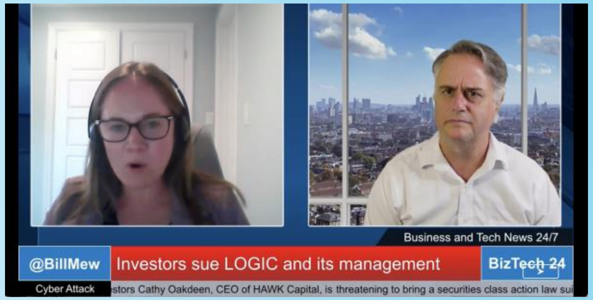
Sergio Bianchi @ChefSergio · 24 s
@betterconnectedhomes My company @dinneratsergios is still waiting on a reply from your Commerce+ membership team. I pay premium subscription costs for the upkeep of my service and livelihood is pinned on your delivery. Please get in touch.

Sergio. #sergios
58 · 21 · 263

George McGregor @George McGregor · 24 s
Wow, even the real Sergio is chipping in!

Peter Frederiksen @PFred · 24 s
@ChefSergio You're an Italian food legend! They need to keep you going! Not sure what I would do without Sergios.


Business and Tech News 24/7
@BillMew
LOGIC hit by Cyber Attack
BizTech 24
Cyber Attack
s, a leading privacy campaigner, is calling for LOGIC to be more open about the crisis.
Reports ar


Business and Tech News 24/7
@BillMew
Investors sue LOGIC and its management
BizTech 24
Cyber Attack
stors Cathy Oakdeen, CEO of HAWK Capital, is threatening to bring a securities class action law sui

thetrust bridge

Our Team

David Clarke **Chief Technology Officer, The Trust Bridge**

Bill Mew (**chair of the IARCC Cyber Working Group**)

David Clarke FBCS, Chief Technology Officer, The Trust Bridge

in the top 15 list of thought leader and influencers by Thinkers 360

- recognised as one of the top 10 influencers by Thompson Reuter most influential thought-leaders on social media, risk management, compliance and regtech in the UK
- features in top 50 list of Global Experts list by Kingston Technology

Bill Mew, Chair of IARCC Cyber Working Group

- Shortlisted for Privacy Champion of the Year in the 2022 Picasso Privacy Awards
- Listed as the world's top expert influencer for Data Privacy and Cybersecurity by Onalytica
- Chair of the IARCC Cyber Working Group
- Formerly on the global leadership team for IBM Financial Services Sector and Cloud Strategist for UKCloud
- Judge on the UK Cloud awards and more

thetrust bridge

Engagement Options

	Basic	Standard	Advanced	Bespoke
Languages			Potential for an extra language as well as English	Potential for multiple languages
Roleplay		Potential for 2 to 3 roles: from CEO, CFO, CLO, CIO, CISO, CMO, Internal Comms and/or External Comms	Potential for multiple roles: from CEO, CFO, CLO, CIO, CISO, CMO, Internal Comms and/or External Comms	Potential for as many roles as required
Scenario	Generic scenario: limited choice and functionality with no customization	Industry-specific scenario: collaborative development of scenario to meet specified sector or industry requirements	Company-specific scenario: collaborative development of scenario to meet specific requirements of client firm	Company-specific scenario with divisional and regional sub-scenarios: to meet specified requirements
Workshop	Short workshop Basic skills transfer Delivered remotely	Half day workshop with skills transfer: can be delivered from client's offices, remotely or hybrid (bringing in remote participants)	Full day workshop with skills transfer: delivered from 1 or more client's offices on hybrid basis (bringing in remote participants)	Potential for multi-day workshop with skills enhanced transfer: delivered as required (on site, remotely or hybrid)

Example of the kind of scenario that we could create for you

Scenario idea:

CLIENT company wanted to automate its insurance processes and a few months ago it acquired InsAI, an insurance AI firm that has built a set of insurance specific data processing modules on top of a well known AI platform. The acquisition went ahead, the client has spent time integrating the new subsidiary with its own systems. So far things have gone well. The AI is used to fast track risk and premium calculations which are then approved by CLIENT's own staff.

Then as the exercise begins a report is presented by the operational risk department that shows that there have been a number of anomalies where policy pricing and claims management appear to be out of kilter. There is a suspicion that the AI has been manipulated or subtly influenced in some way. This should not be a problem as the system allows CLIENT to bypass the AI on whatever business lines it chooses or to suspend the AI entirely and return to its existing systems at any time.

CLIENT execs take the decision to bypass or suspend the AI at which point they find that there has not only been an intruder on the system that has indeed been manipulating the AI, but that the intruder has also obtained administration access to other parts of the system. When they try to bypassed or suspended the AI, this is taken by the intruder as an indication that he has been discovered and so he switches into a ransomware mode, triggering malware that he has already inserted across the company's entire systems.

Investigation indicates that while the system was built on a well known AI platform that is known to be secure, the development tools used to craft the specific insurance functionality had been compromised - long before the acquisition - and this had not been picked up during the M&A due diligence process.

A series of actions unfold:

- CLIENT discovers that it has been locked out of its systems all of a sudden - including IP telephony and email - both of which InsAI uses
- The malware is triggered and data is either encrypted or file names are changed such that data cannot be found or accessed
- The backups for InsAI are found to have also been compromised
- InsAI has a pre-existing cyber insurance contract that had been in existence prior to the acquisition, but the insurer is refusing to honour the claim due to a contractual technicality
- The intruder has access to a great deal of sensitive personal and financial data and threatens to start leaking it unless a ransom is paid promptly for the decrypt keys

This would be an ideal scenario as we can make up what we like about the acquired organisation InsAI with whatever hack history we like.

“Don't wait until a crisis occurs before thinking of crisis management. It is like waiting until you are drowning before thinking of learning to swim.”

“It takes a lifetime to build a reputation and only seconds to destroy one.”

THANK YOU

Penny Heyes

+44(0) 7768 962 480

penny.heyes@thetrustbridge.com

www.thetrustbridge.co.uk

thetrust bridge™