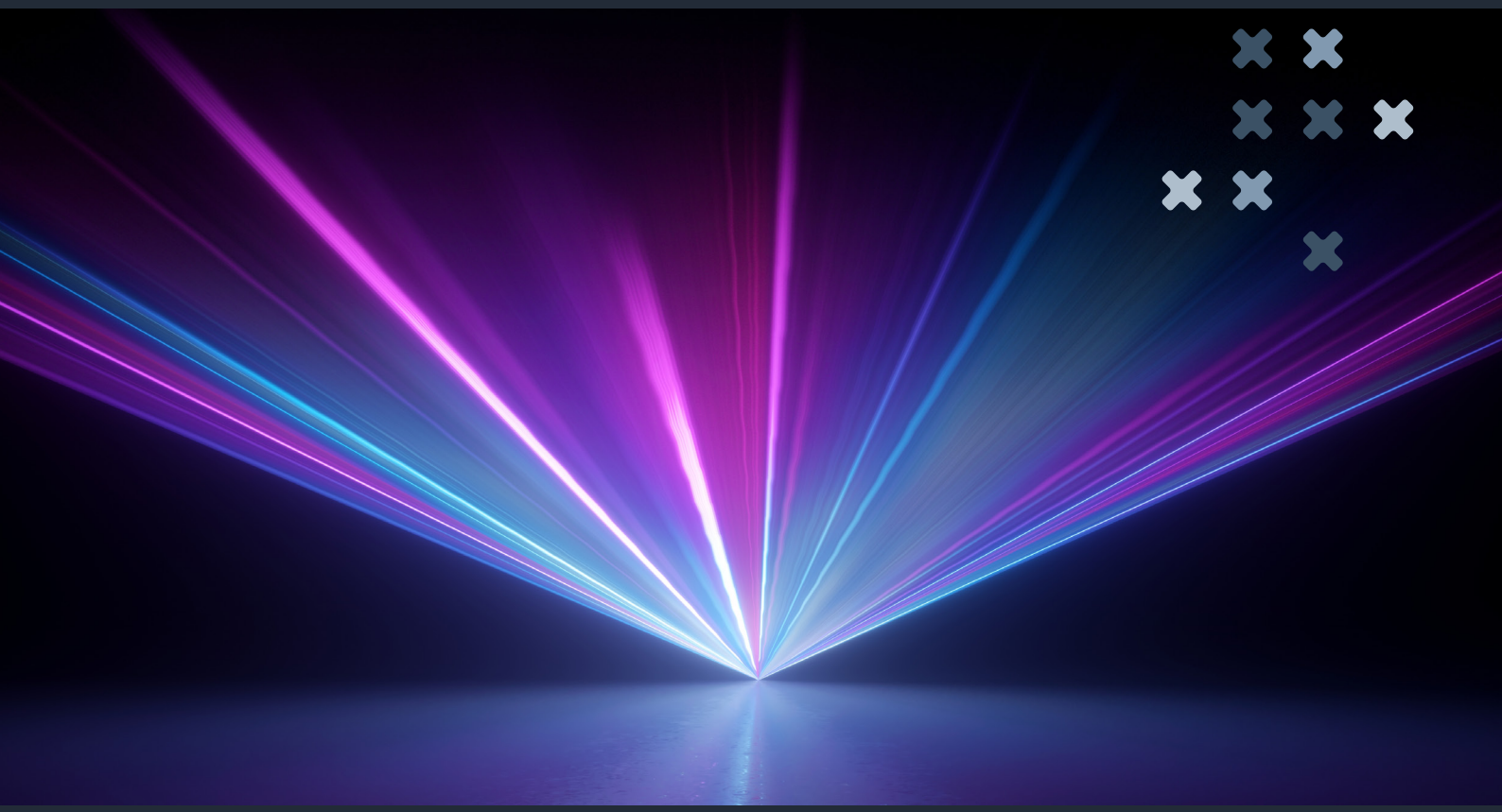
SECURE IMPACT | dwf



THE CISO's GUIDE

The 6 critical aspects of incident response

What works and what makes breaches worse

www.secure-impact.com

“These are the practical steps that you can apply now to make sure you limit damage to your reputation and achieve the best outcome with regulators. Don’t make the mistake of waiting until the house is on fire!”

James Lyne

If you would like to discuss this e-book in more detail, please contact Giorgia Cacace directly at gcacace@secure-impact.com

Introduction

Incidents and breaches are undeniably one of the most stressful situations a security team can be faced with. Over the last 12 months, 39% of UK businesses were reported to have been the target of a cyber-attack[1].

With statistics such as these it seems inevitable that most businesses will become the target of cyber criminals at one point or another, and it is more important than ever that you are prepared and know how to respond.

Incident response is about limiting the bleeding and stopping it, using the right practices in a calm and methodical approach to stop the attacker, and limiting your exposure. Building great resilience to protect your reputation when faced with a breach will involve a clear and well-practiced incident response plan, technical competence and working with legal counsel to manage your process of discoverability. Many teams have a policy in place, but has it been practiced recently? Have all relevant team members been included in the simulation? Are you inviting legal and regulatory risks through your current security practices?

We heard from the audience during a recent webinar co-hosted with DWF, and their top concerns were **how to communicate to stakeholders and clients during a breach** (44%) and **whether their teams were practiced enough** (37%), with the key objective being to **prevent reputational damage** (32%).

This e-book answers these concerns and provides practical strategies that you can (and should!) implement now. Take proactive action now – don't wait until you're faced with a breach!

The 6 critical aspects of incident response:

1. Practice makes perfect.
2. Get to know your allies.
3. Technical considerations.
4. Manage your legal & regulatory risk.
5. Protect your reputation through clear communications.
6. Don't make the mistake of doing procurement during a breach!

This e-book includes valuable insights gained from a recent CISO roundtable attended by a group of seasoned security leaders, as well as experts from Secure Impact & DWF.

1. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

1. Practice makes perfect

“Good companies get hacked; mistakes happen. To put yourself in the best position to succeed when faced with a cyber incident, practice really is the answer.”
Giorgia Cacace

The definition of a crisis is that you can’t predict it – but you can plan for it.

When faced with an incident, you will likely have a huge number of priorities that all need to be sorted immediately, at the same time. These include containing the incident, continuing operations, producing clear communications to worried clients and stakeholders, and managing your company reputation throughout. None of this can be achieved without a clear plan in place – a clear plan that has been practiced will make this ten times easier.

Your incident response plan should not be a tick box exercise, and no one should be learning how to respond in the middle of a breach! Tabletop exercises create an environment to clearly define and test each role and iron out any issues in advance –

and this is often the difference between a good or bad response. These simulations should involve all relevant stakeholders, although as one security expert commented, “it is often hard to make sure they all turn up.” It can be helpful to have these simulations run by a third party who are experienced at spotting the holes, and to establish the credibility of the exercise to ensure everyone turns up on the day.

Being able to prove that you have an established plan in place can also help you to maintain your reputation if faced with a breach. A common problem for businesses is often the community’s reaction to sharing their processes and timeline – having a robust and practiced plan will frame you as a victim, rather than negligent, to clients, stakeholders, and the wider community. Regulators will also want to know whether you have done everything you possibly can to minimise the damage and protect your business. In the long run, practicing your response plan now will help you to avoid losing credibility and trust if the worst happens.

Practical steps to take now:

1. **Do you have an incident response plan and when did you last review it?** Make sure you have a specific and detailed incident response plan outlining what actions you should take in each of the most likely scenarios. This should also include key decision makers and established processes to be followed.

2. **Organise tabletop exercises to practice and test your plan.** If you go external for this, you will need a team who are experienced at running these simulations, at spotting areas for improvement, and can work with your team to make sure everyone is properly trained and prepared. The SI team are experienced at running these exercises with businesses.

3. **Cyber insurance – do you know what your policy covers?** What invalidates your policy? Who makes the decision about whether you should pay a ransom?

2. Get to know your allies

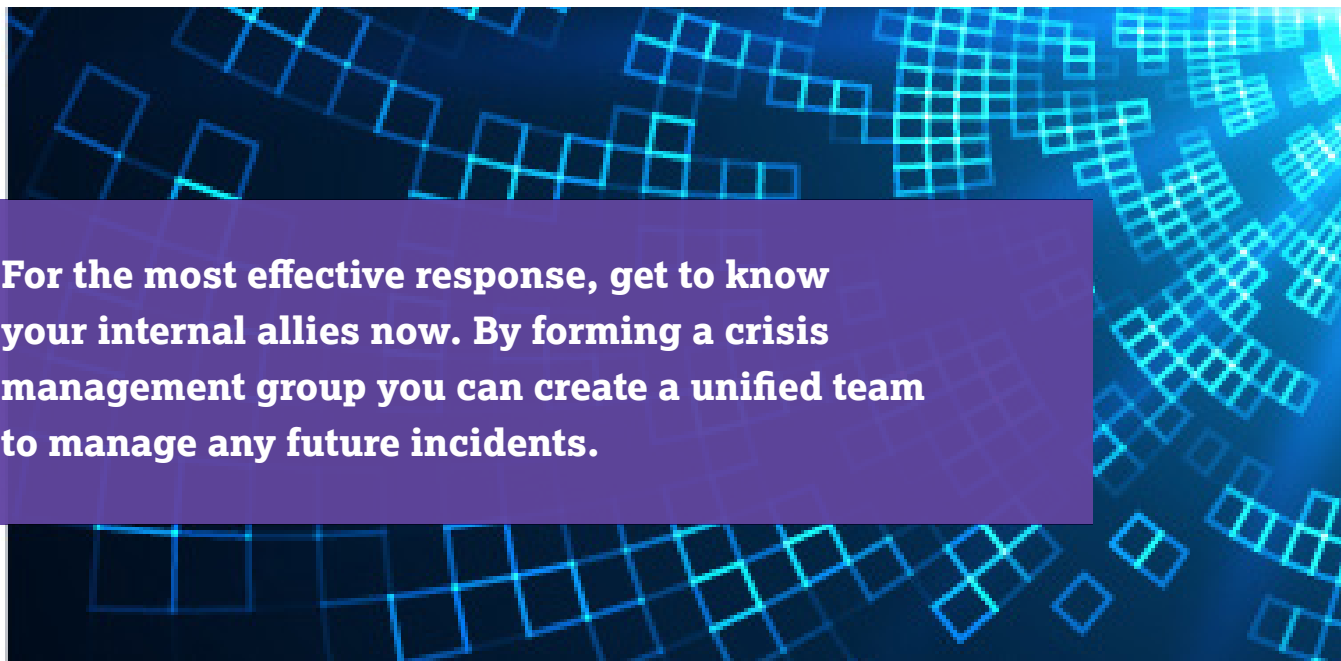
"Incidents are not an IT or Cyber problem – they are an entire business problem."
Tom Fawcus Gibbs

Incident response should never be left to one individual or one team – they are a business wide problem that requires a joined-up response, and internal collaboration is key. However, as commented by one roundtable attendee, *"cyber security is the mythical beast that no one understands"*.

It has therefore become an important part of the CISO or security leader's role to raise awareness and break down this perception that an incident is simply a cyber security issue. One way to do this is to provide parallels to other business processes. If an incident occurs and all systems are down, how will HR pay employees? If communication channels have been breached, how will senior management communicate with the wider company?

For the most effective response, get to know your internal allies now. By forming a crisis management group you can create a unified team to manage any future incidents.

Practicing your plan is a good way of getting to know each other better and supports a more joined up approach. This preparation benefits everyone when things go wrong, and also allows you to go to the board together rather than in isolation. By avoiding silos you can create better and



For the most effective response, get to know your internal allies now. By forming a crisis management group you can create a unified team to manage any future incidents.

more effective working practices. Have you spoken to your legal team, DPO or chief risk officer recently?

One interesting point raised at our roundtable was whether the CEO should be on a crisis management committee. The answer given by most was no, as in a crisis they will have far too many issues to be concerned with, and the response committee should instead empower the management layer down. By trying to include the CEO in a planned simulation, you are also increasing the chance of it being rescheduled or cancelled due to their limited availability.

Practical steps to take now:

1. **Get to know your internal allies.** If you don't know them already, get to know which of your colleagues will play a critical role in a breach.

2. **Form your own crisis management group including all relevant stakeholders.** Depending on your business structure this could include; Legal, CISO, IT, Risk, DPO, HR, PR and admin support.

3. **Decide how you will assemble and communicate during a breach.** How will you contact each other if your email or Teams/ Slack channels are down or compromised? What should and shouldn't you discuss? These are basics steps but can become basic mistakes during an incident.

3. Technical considerations

Poorly configured systems and lack of technical support can often cause the impact of an incident to be far greater than it should've been.

Implementing the tips below will help your business to be prepared, but if you're at all unsure you should consult your internal team, or contact a technical specialist – please reach out if you'd like to discuss.

The technical set up of your systems and processes can greatly improve your chances of successfully remediating and investigating a breach. There are several processes that you should consider now to put yourself in the best position when faced with a cyber incident.

- Ransomware sees a year-on-year surge, make sure you plan for it. Check your backups are regular and robust enough to mitigate the impact.
- If an incident occurs you should involve your digital forensics team as soon as possible, or, even better, include forensics as part of your IR response plan. They should be contacted as soon as an incident is identified to ensure evidence does not erode.
- Logging is important in a digital forensics investigation, and where possible, logs should be centralised, and use a sensible timestamp (UTC is strongly recommended). In your preparation, think about what logs you are collecting (or not collecting), and how long they will be stored for. If you are not storing logs for long enough, then why collect them in the first place?
- To reduce the possibility of a repeat incident, learnings or suggestions can be taken from a report or debriefing and can influence procedure and future training.
- Many incidents are caused or enabled by human error, and training and quality communications for all employees can reduce these errors.

The technical set up of your systems and processes can greatly improve your chances of successfully remediating and investigating a breach.

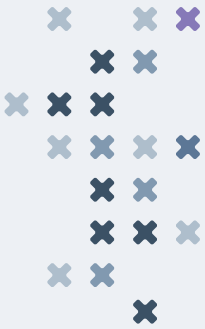
Practical steps to take now:

1 **Perform a test of your backups**, pick several areas key to your organisation and perform tests. Tests can be potentially disruptive so consider down time and communication.

2 **Check your logs.** What are you logging and why? Perform an exercise where you hypothesise an attack, discuss what should be generated and test to see if these logs are being generated. How easy was it to retrieve the logs? How easily could they be queried? Could this be done quickly in a real incident?

3 **Increase logging.** Windows default logging can be lacking, look to increase logging. There are Windows tools such as ***Sysmon*** which can greatly increase logging. Roll this out on key systems and systems with outward-facing services, though if CPU and storage capacity permit, it is recommended to utilise increased logging across the organisation. This is not just pertinent to Windows machines; Linux has tools such as ***auditd*** to increase logging.

4 **Perform a purple team scenario** where you have a red and blue team simulate an attack pertinent to your environment, then collaborate to investigate this attack. Could this attack be prevented? Was it detected? Did the attack generate logs? How would you respond to this attack and did your Incident Response plan work?



4. Manage your legal & regulatory risk

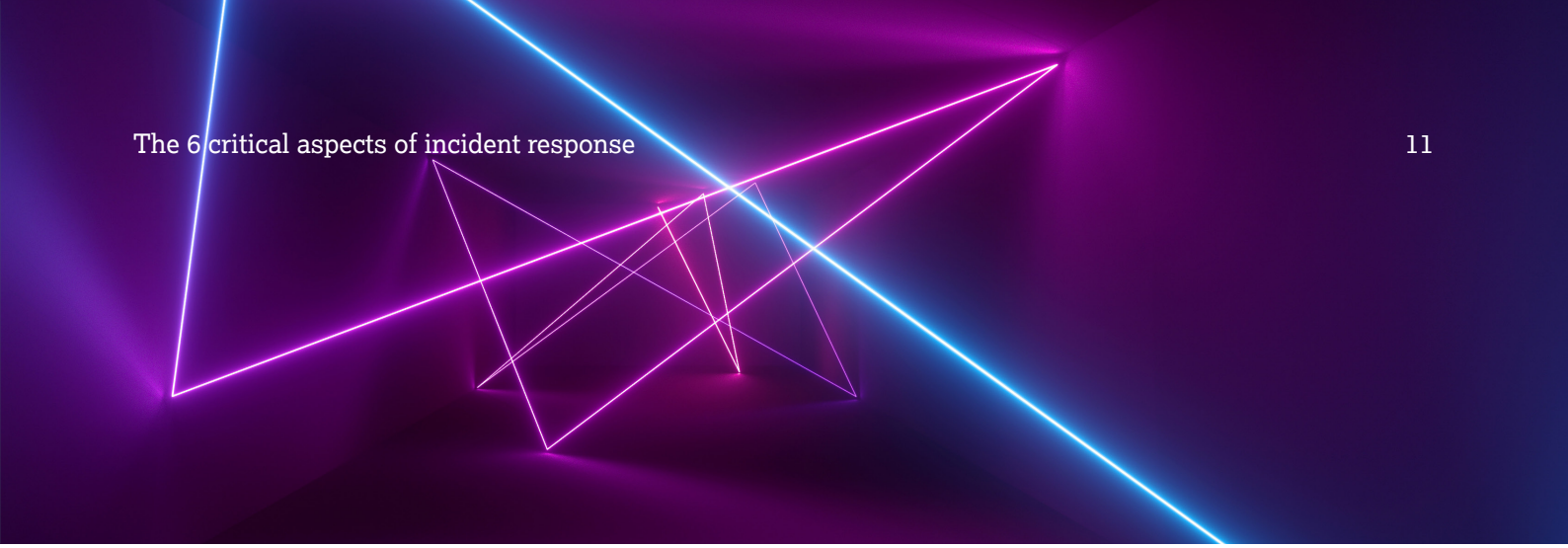
"Do you know what's sitting in your drawer? Have you remedied penetration test and audit findings? Don't leave 'smoking guns' lying around which may become disclosable during regulatory investigations and litigation."
Richard Hall, DWF

CISOs are in the business of making 'smoking guns'. Security leaders are programmed to look for holes and vulnerabilities in order to fix them and are constantly chasing bad news in efforts to make improvements. This can come back to bite however, if you are faced with a breach and the subsequent regulatory investigation and/or litigation. So, what are the best tactics to use from a legal perspective? How can you have the candid conversations without landing yourself in hot water further down the line?

Framing the conversation
You of course need to talk about your business risks, but in the right way. It's all about framing the conversation and controlling the narrative. To do this, build a 'good news' file of all of the remediation and proactive actions you've taken as a team. The document should describe how you processed and remediated vulnerabilities, which will help with regulators if you are investigated for a breach. Building up a story about your good work will show that you took every reasonable step to protect your systems and data – you invested in the highest risk areas and are able to demonstrate that.

Address the gaps!
As explained by Richard Hall (DWF), *"there are two types of businesses – those that do a pen-test and make serious efforts to address the red flags and close the holes. And then there are those that do a pen-test and do nothing,"* although this often depends on the quality of penetration testing vendor used! His advice is to address your red flags before moving on to your next penetration test or obtaining further reports (instructing a vendor who can help fix the gaps rather than just point them out can help here). Obtaining report after report containing more and more red flags, will not help if the red flags already highlighted have not been addressed.

Remember that if your organisation is faced with an investigation, one of the first things a regulator may request is your audit and/or pen test reports. If an unaddressed vulnerability is highlighted that is attributable to the root cause of an incident, you are likely to find yourself in hot water. In summary, make sure there are no reports lying around with old red flags that have not been addressed and don't simply build on top of them with further reports without purposeful activity planned off the back of them.



Business chat / messaging systems & emails are easy pickings for regulators.
Ensure all security related discussions are conducted through approved communication channels and legal are involved where necessary for the purposes of managing privilege. Be careful what you put in writing, you don't know who is going to be looking at it later – no loose comments on chat systems or over email!

You won't always be required to submit your full IR report!
You can dig yourself a hole early on through over-disclosure and by making unnecessary admissions to regulators. Work with your legal and security team as early as possible if faced with an incident to ensure legal privilege and document control.

Practical steps to take now:

1 **Check what is lying in your drawer.** This could be purposeless or non-strategic penetration test reports, audit reports, due diligence questionnaires, and other documents. They could have been created by predecessors or other teams, so speak with your General Counsel, DPO or IT team. A penetration test reflects a point in time, and if it has expired then your business has moved on and the report should be addressed or deleted once standard retention periods have elapsed.

2 **Choose your penetration testers wisely.** Many vendors offering penetration tests today are going to run a commoditised scan and produce a report which will not inspire or communicate the targeted action from your team to remediate in a high impact way. High-level non-specific findings are unhelpful and can be attributed to a wider range of issues if you suffer an incident. The SI team can help if you want to learn more.

3 **Create a clear document retention policy.** Have the conversation internally and create a policy that outlines which documents you should keep, how long you need to keep them, and which documents even need to be on site. Don't keep old files that are unnecessary and past their retention period. Remember if it exists, it may be subject to discovery and disclosure during an investigation or litigation!

4 **Keep communication channels secure.** Speak to your legal counsel to confirm when privilege applies, the simple rules to follow to increase the chances of privilege being applicable and what channels to use.

5 **Put together a 'good news' pack.** Keep a file that documents all remediation action you have taken, your decision making, security processes and good news stories that advocate your team. This may be extremely important later in demonstrating whether or not the organisation has carried out reasonable actions to protect data subjects.

5. Protect your reputation through clear communications

"We've all seen those situations where an unprepared executive gets interviewed following a breach and proceeds to damage their company reputation with unclear and confusing messaging. To avoid this, make sure you have a clear communications structure, and PR support and training where possible."

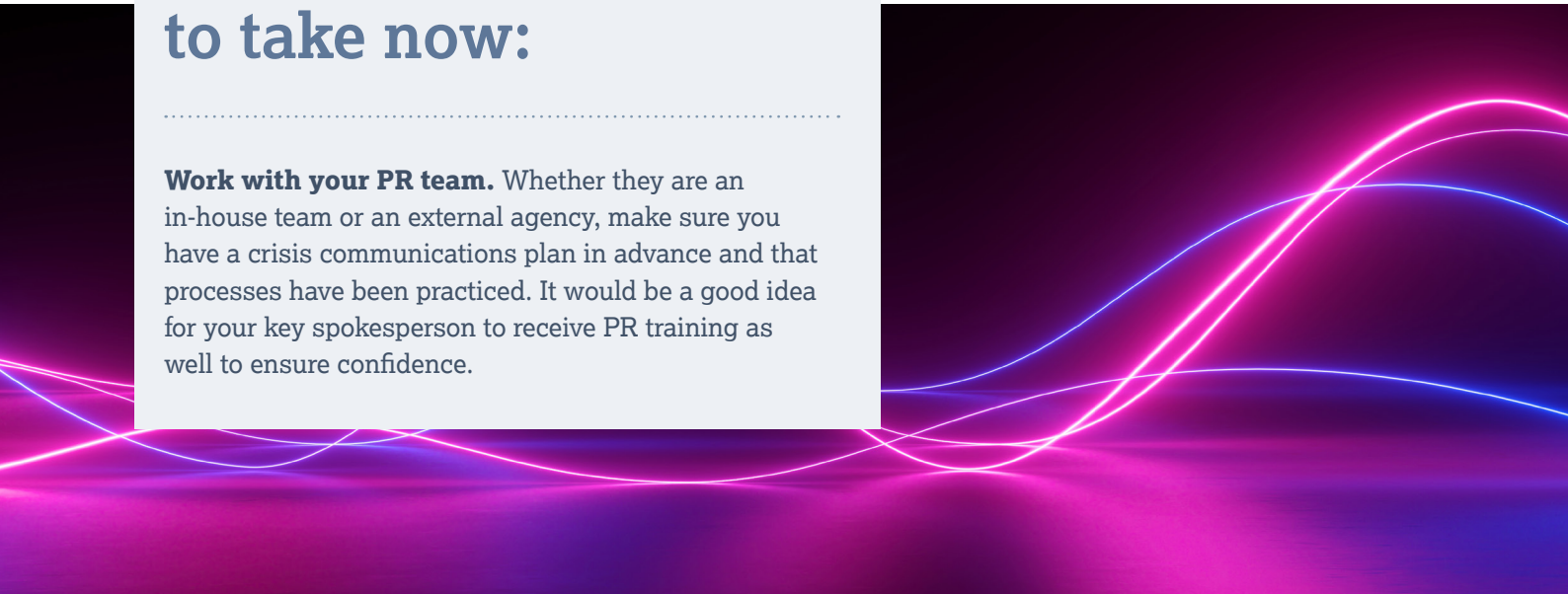
James Lyne

The communications you make around a breach, whether internal or external, can make or break your reputation, which is often the biggest impact of an incident. It can define whether you are viewed as negligent or merely a victim who is in control of the situation. It can instil confidence in your employees, clients, and stakeholders, or can tarnish your reputation and break down trusted relationships.

It is important to have the right communications hierarchy in place. When should PR be contacted? Who is your key spokesperson? What needs to be confirmed before any external messages are sent out? In a crisis situation, well intending people can send out the wrong communications, so you need the right structure in place early on. An under informed team can undermine customer confidence so you need defined processes and communications, and to have practiced them.

A practical step to take now:

Work with your PR team. Whether they are an in-house team or an external agency, make sure you have a crisis communications plan in advance and that processes have been practiced. It would be a good idea for your key spokesperson to receive PR training as well to ensure confidence.



6. Don’t make the mistake of doing procurement during a breach!

“Most businesses don’t build their security teams staffed and ready for a crisis, so bringing in an experienced team can support you in achieving positive outcomes.”
Giorgia Cacace

Even if your internal team are prepped and ready, a cyber incident can sometimes take weeks to resolve, and involves a team working over numerous weekends. Having back-up support can be invaluable in these situations.

A team who has experienced this many times before understands the different tactics that can be used to stop your attacker. This can vary depending on the attack vector, and they will know when to take action, and when to stand back and wait. They can also help you to produce the right documentation that may be required by legal and regulatory bodies.

A practical step to take now:

Make sure you have a DFIR provider in place. We work with our clients to prepare for the unexpected. We can help you to build up your defences and run tabletop exercises to practice your IR plan. If you are faced with a cyber-attack, our team have experience in law enforcement and offer a highly disciplined approach to uncovering and interpreting evidence. They have in-depth understanding of legal privilege and can act as credible expert witnesses in court.

The last thing you want to be doing is working out who your incident response or digital forensics team are in the middle of a breach. A top tip is to choose a partner with expert witness capabilities and a partner that knows chain of custody, as this will be invaluable if your case ends up going to court.

Next steps – how we can help

If you currently have an IR plan in place...

We can help you to practice through tabletop exercises and tease out specific areas for improvement with actionable road maps to make these impactful improvements. We can design and run hands-on exercises in real-world environments to prepare your team for an incident. This can be a highly rewarding opportunity to build relationships, clarify roles and responsibilities, map out any vulnerabilities, and then test these in one or more scenarios.

If you don't currently have an IR plan in place...

We can work with you to put together a robust IR strategy document, then help you test it. Our consultants will work with you to really understand your team and company's specific issues, the trends in your industry and region, and against your upcoming business milestones and objectives. Our aim will be to collaboratively assess the most high target, cost efficient approach to building up your business's defences and partner to produce a clear response strategy, providing you with the peace of mind you and your stakeholders need.

If you recently had an incident and want to make proactive changes...

Our digital forensics team can investigate the root cause of the incident to prevent a similar attack from happening again. Made up of ex-law enforcement and military, our digital forensics team have a highly disciplined approach to uncovering and interpreting evidence, its validation, preservation and documentation. They will provide an actionable report at the end with clear next steps for improving your security posture.

If you don't currently have an incident response or digital forensics provider in place, but want to be prepared for the inevitable...

Please contact us for an initial conversation about how we can help! In an industry that's noisy, commoditised and compliance-driven, our mission is to add value and create real business outcomes with every engagement. We're excited to help you with your team's most pressing security needs so please do get in touch!

Key contacts

Get in touch with our team at hello@secure-impact.com

James Lyne
Founder

Giorgia Cacace
General Manager

David Barr
Principal CIRT Consultant

Tom Fawcus-Gibbs
VP of Technology

Richard Hall
Director, DWF

Additional resources

The 5 biggest mistakes businesses make before, during and after a breach

Top 5 mistakes in incident response

SECURE IMPACT

Your security team.

Your security team.

We understand you have real business challenges which likely won't be solved with commoditised scans, tick box exercises or generic reports. Our GIAC-certified team can help create real business outcomes for you and your team through collaborative offensive and defensive engagements.

From penetration testing to digital forensics and incident response, we promise services which are business-oriented, bespoke to your risk profile, and geared to achieving your security objectives.

We partner with CISOs and security teams from the FTSE 100 to VC-backed scale-ups, creating shared learning outcomes for our clients, and developing a roadmap to improve their cyber security maturity.

Secure Impact Ltd.
The Old Bull Pens, Sezincote, Moreton-in-Marsh, Gloucestershire, GL56 9AW

Want to discuss how we can help your business? Contact us to learn more.

hello@secure-impact.com | +44 (0)20 45514730

www.secure-impact.com

SM22-709