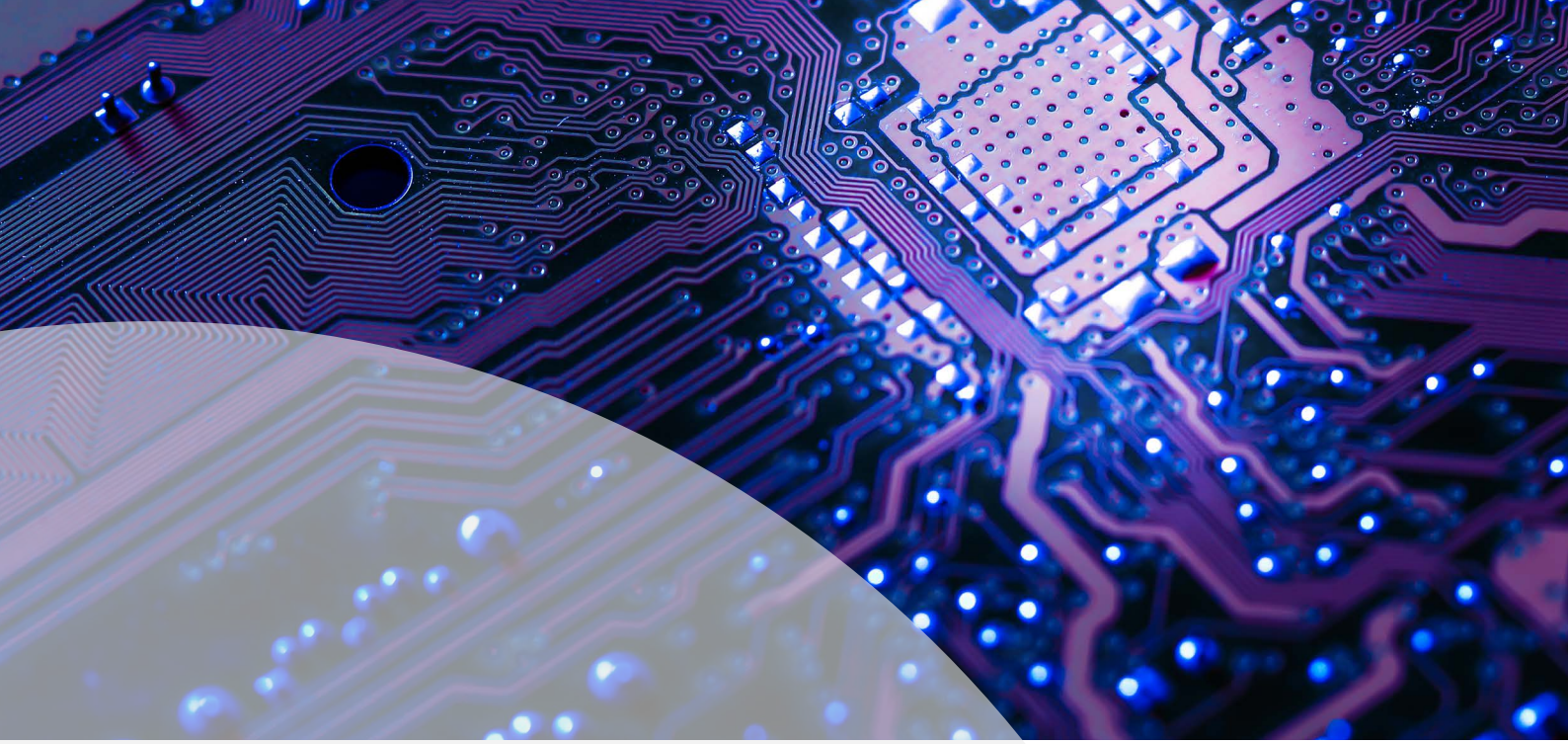
bsi.

Inspiring trust for a more resilient world

Manage data breaches – Six steps to keep your organization secure



Executive summary

Data breaches are on the rise. According to Cybersecurity Ventures, a data breach occurs every 14 seconds, down from every 40 seconds in 2016 and by 2021 will occur every 11 seconds. To put that into perspective, in one day there are approx. 8000 data breaches and in one week over 55000!

In the same report cybercrime will cost the global economy a staggering $6trillion, yes that is a "t" and cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades.

Now with the emergence of the largest proof of concept project in the digital world – half of the world suddenly working remotely – the threat landscape takes on a new dimension; cybercriminals taking advantage of the COVID19 pandemic and media frenzy.

With the volume of content and media outpour since the end of February, scammers have taken this time for solidarity as an opportunity to scam, hack and cause mayhem across the digital landscape. These are coming in many forms but none more so than phishing and social engineering scams, sale of fraudulent or counterfeit goods and misinformation / fake news causing mass consternation.

So, what should organizations do if they have a data breach? According to BSI, there are six stages of a data security or data privacy breach that incident response teams should follow to help detect and ultimately manage a data breach and provide remediation that can ensure an enhanced state of information resilience.

1. **Preparing for a data breach**: Have you put the right governance structure in place, with the correct resources and toolsets?
2. **Identifying a data breach**: Can your team respond to security alerts and determine if there has been a potential incident and ultimately a data breach?
3. **Containing a breach**: Are there plans in place with the rights resources to stop a data breach.
4. **Eradicating a breach**: Do you have the right tools to remove the vulnerability that caused the breach?
5. **Restoring from a breach**: Are you able to recover your systems in near real time?
6. **Lessons learnt from a breach**: Is there a review mechanism to assess your team's response and identify if improvement can be made?

01
Preparing for a data breach

Preparing for the inevitable. An incident response plan should define the roles, responsibilities and activities that need to be carried out for every member of your team. The list below is a useful preparation guide:

- Up to date risk register of information security risks covering all assets
- Implement security tools to detect potential breaches
- Understand and document the scope and coverage of your security tools
- Have a defined incident response plan, with actions defined for when a breach is detected
- Document the parameters that will determine the severity of the breach and the potential impact on the business and affected individuals.
- Have plans to alert key stakeholders, senior management, partners, authorities and clients
- Create playbooks to handle the most common types of breaches scenarios
- Prepare templates to capture key events and activities as they occur during the incident
- Ensure the ability to react when roles are outsources to different cloud environments
- Carry out a business impact assessment covering all your services and systems to determine the priority in the event of multiple system breaches
- Security governance structure

Our virtual services include:

- Incident management
- Penetration testing
- Vulnerability management
- Red teaming
- Cloud security solutions

"Prevention is better than cure rings true when it comes to preparing for a data breach. Having an actionable incident response plan in place helps organizations action the steps to take when a data breach occurs"

Inés Rubio
Head of Information Management and Incident Response eDiscovery and Forensics
Email: ines.rubio@bsigroup.com

An incident response plan should define the roles, responsibilities and activities that need to be carried out for every member of your team.

02
Identifying a data breach

Finding out where the breach occured and to check if data was compromised. The ability to respond to a security event, detect a security incident and then identify that a data breach has occurred depends on how your team have configured the security tools to detect for Indicators of Compromise (IoC) and alert as appropriate.

Make sure to assess the following:

- Maturity of your security organization (outsourced or inhouse)
- Configuration and coverage of the security tools
- Deployment of an event correlation tool
- Incident Response Team structure defined
- Awareness of your security risks and risk appetite
- Understanding of your network and associated data flows
- Geographical coverage

Whenever there is a potential or actual breach, the security incident response plan should be activated, and the incident response team should be called to investigate further.

Our virtual services include:

- Risk assessments
- Forensics
- Disaster recovery
- Business continuity planning

"Should you have a data breach, it is imperative that the organizaiton is ready and has the right remediation in place to ensure that there is the sufficient tools in place to identify the breach, check if data was compromised and if the business systems can continue in the event of adversity."

Stephen Bowes
Global Practice Director - Security and Information Technologies
Email: stephen.bowes@bsigroup.com

Whenever there is a potential or actual breach, the security incident response plan should be activated, and the incident response team should be called to investigate further.

03
Contain and eradicate the data breach

Isolate the incident and ensuring no further vulnerabilities are exploitable. When your team has identified a breach has occurred, the next step is to stop any further egress of data and ensure that any potential vulnerabilities have been removed. Ensure no additional backdoors have been added to the system so that your organization can return to business as usual.

To help in carrying out the containment and eradication process, the team should follow run books. These are the defined set of instructions that ensure the right steps are taken in the correct order to ensure that the breach is contained quickly, the relevant authorities and stakeholders are informed, and evidence is collected. However, if no runbook has been created for the actual breach scenario, then one of the first things your incident response team should do, is define a plan and identify a course of actions (CoA) to contain and eradicate the breach.

The CoA should cover both governance and technical actions. You could consider the following as a potential set of actions (this is not a complete set of actions):

- Determine what information and assets have been compromised
- Identify if you or the Cloud Service Provider (CSP) are responsible for managing the breach
- Identify what actions were carried out to contain the breach in the short term
- Identify and confirm notification obligations to data protection authorities
- Assess the impact on the fundamental rights and freedoms of the affected data subjects
- Clarify whether the breach is one of confidentiality, integrity or availability
- Prioritize next steps based on business and regulatory requirements
- Escalate to senior management and inform them the breach has occurred
- Communicate the information security incident and relevant details to individuals or others that may be affected if required
- Ensure that the incident response team document all their activities for later analysis
- Notify relevant regulators within the appropriate time scales if required

Our virtual services include:

- eDiscovery
- Incident response
- Data protection services
- DPO services
- Online training
- End user security awareness

"The containment and eradication of the data breach is as important as the identification of the breach. Organizations should have a sufficient course of action that determines if there has been a compromise, the source of the breach, what are the risks, impact assessments, a communications plan to relevant stakeholders and business continuity planning measures in place."

St. John Harold
Senior Cyber, Risk and Advisory Consultant
Email: St.John.Harold@bsigroup.com

When your team has identified a breach has occurred, the next step is to stop any further egress of data and ensure that any potential vulnerabilities have been removed

04
Restoring from a breach

It is possible to recover from a breach and returning operations to business-as-usual is the aim. After a breach has been contained, consider the best way to restore assets and protect your network to prevent future security breaches and focus on necessary measures to rebuild consumer (and/or employee) trust in your brand or products.

From an IT perspective, recovering from a breach can involve the following actions:

- Restoring systems and datasets from backup copies
- Building replacement systems
- Utilizing a BCP/failover system

Some organizations may be too keen to revert to business-as-usual as quickly as possible and restore systems from backup without proper or robust evidence capture. This can compromise the resulting investigations and analysis leading to insufficient conclusions or inadequate lessons learned. It is important that the requirements for capturing evidence and maintaining the integrity of this evidence are carefully considered, especially if any subsequent litigation or restorative actions are undertaken. Careful examination of the attack method, vectors and finding out how the attacker succeeded, leads to the identification of gaps in your cybersecurity and data protection framework that once remediated will help reduce the likelihood of future breaches.

Our virtual services include:

- Backup systems
- Recovery services
- Data protection impact assessments
- Online security and privacy training
- End user security awareness

Returning to business as usual post-breach should be the primary aim to reduce disruption and reductions in productivity. Backups play an important role, enabling an organization to restore systems and datasets from backup copies"

Michael Green
Senior Cloud Security Consultant
Email: michael.green@bsigroup.com

Some organizations may be too keen to revert to business-as-usual as quickly as possible and restore systems from backup without proper or robust evidence capture.

05
Post incident review

Undertaking a post-incident review allows an organization to carefully understand each part of an incident, and the key decisions, remediation steps and actions are taken in detail. A good post-incident review exposes network or technical vulnerabilities, internal control weaknesses, policy issues, human error, or even just simple mistakes that may have led to or exacerbated the compromise, or indeed affected the ability to contain, eradicate and recover efficiently.

Organizations should carry out this review to assess the incident management process and to determine:

- How quickly actions were taken to identify, respond to and recover from the incident
- How long the attackers were in systems before detection
- What actions attackers took and planned to take
- The level of protection maintained over critical systems and confidential information, for example personal data, during the incident
- How well staff and management performed in dealing with the incident
- If any steps or actions taken might have inhibited the recovery
- What opportunities for improvement may exist within the existing incident management process?
- Whether relevant regulatory or statutory reporting deadlines were sufficiently met

Our virtual services include:

- Incident response management plan
- Threat intelligence
- Vulnerability assessments and management
- End user security awareness programmes

Over 90% of cyber-attacks begin with a phishing attack, so ensuring employees are trained up to anticipate, identify, report on and manage phishing attacks is paramount to the information resilience of an organization, and whilst preventing cyber-attacks that may lead to data breaches in the future."

Richard Lambe
Senior Security Awareness Consultant
Email: richard.lambe@bsigroup.com

Undertaking a post-incident review allows an organization to carefully understand each part of an incident, and the key decisions, remediation steps and actions are taken in detail.

06
Lessons learnt due to a data breach

One of the best ways to understand how you can protect your data is by reviewing the "lessons learned" from previous incidents. A key step is to perform a 'root cause analysis' to determine how the incident occurred, if it was due to a human failing or was it a system failure such as a misconfiguration, or zero-day vulnerability. Once the root cause has been identified it is possible to resolve the issues.

Key steps to consider during the breach process:

- Have the discussions and decisions during the breach process been documented?
- Are your current policies or processes suitable for the organization, considering the breach?
- Was lack of training and awareness instrumental in causing the incident?
- Confirm if any changes to policy or process as a result if the lessons learnt, have been shared across all the business, and not just within your IR team?
- What regulatory, statutory or contractual obligations apply during the incident?
- Are there minimum or maximum reporting deadlines, or thresholds?

Our virtual services include:

- Impact assessments
- Phishing simulations
- Testing services
- Cyber, risk and advisory services
- Online training
- End user security awareness programmes

"Ensuring that your organization is achieving a state of information resilience, organizations needs to address their cybersecurity, data privacy and security awareness requirements. Data breaches are no longer a matter of "if" they happen, rather a matter of "when" they happen so ensuring that organizations have the right protocols and procedures in place will give them a state of information resilience to ensure their sustainability and that they thrive over the long term and can withstand the test of time."

Stephen O'Boyle
Global Practice Director - Cyber, Risk and Advisory
Email: stephen.oboyle@bsigroup.com

One of the best ways to understand how you can protect your data is by reviewing the "lessons learned" from previous incidents.

Conclusion

Irrespective of whether organizations are remote working or office based, organizations need to be prepared for data breaches all the time and having protocols in place that prepares for their inevitable. To better understand why and how a data breach occurred, it is necessary to reflect on two intrinsically linked components: the human element and the technological element.

Inadequate management or configuration of the technology stack increases the risk of an information security breach, and when combined with the unpredictable behaviour of the human, attackers are presented with almost perfect opportunities to exploit weaknesses and cause a data breach.

BSI is uniquely placed to help reduce the risk of a data breach occurring and manage the data breach when it occurs. We can assist your teams by developing a layered lifecycle approach to the data breach management from risk assessments, controls implementation, ongoing monitoring, and testing control effectiveness within the context of your environment. We can also support your organization's capabilities to respond to the breach, this includes incident response management, forensics investigation, e-Discovery and support, and advising on data protection compliance obligations such as assessing the impact of a personal data breach, and the data subject or supervisory authority notifications.

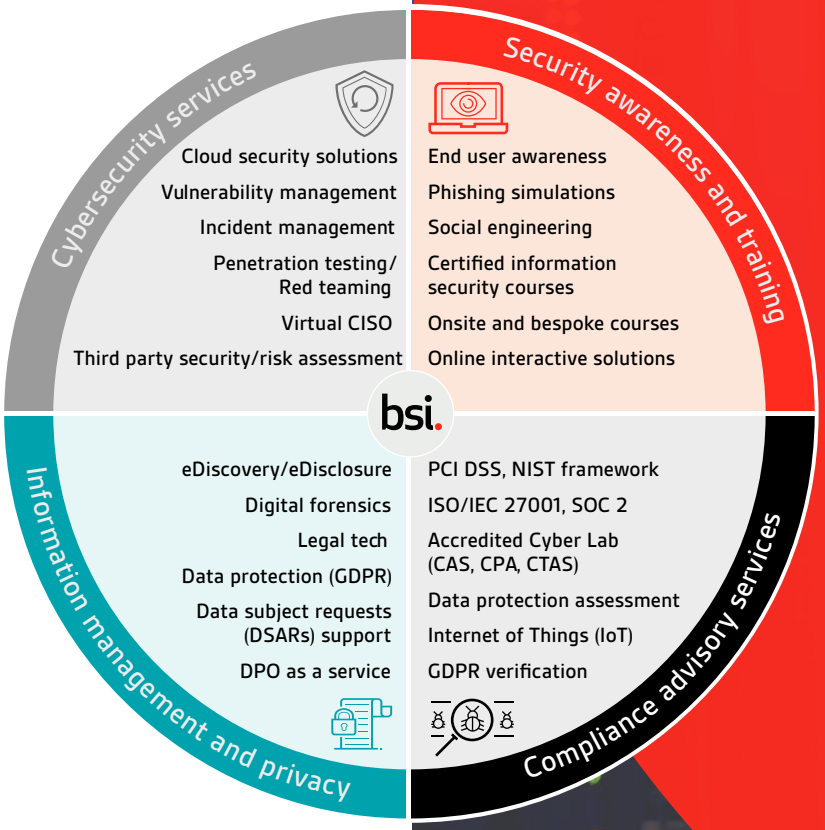
Disclaimer
BSI is an accredited Certification Body for Management System Certification and Product certification. No BSI Group company may provide management system consultancy or product consultancy that could be in breach of accreditation requirements. Clients who have received any form of management system consultancy or product consultancy from any BSI Group company are unable to have BSI certification services within a 2 year period following completion of consultancy.

How to deal with a data breach: 6 steps to keep your organization safe
Call: +1 800 862 4977 (US) / +44 345 222 1711 (UK) / +353 1 210 1711 (IE)
Email: cyber@bsigroup.com

Protect your information, people and reputation with BSI

Expertise lies at the heart of what we do. As trusted advisors of best practice, we empower you to keep your business safe through a diverse portfolio of information security solutions. Whether it's certification, product testing, or consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Cybersecurity and Information Resilience Services include:



Our expertise is accredited by:

Find out more

EMEA
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie

UK
+44 345 222 1711
cyber@bsigroup.com
bsigroup.com/cyber-uk

US
+1 800 862 4977
cyber.us@bsigroup.com
bsigroup.com/cyber-us

bsi.

Subscribe to our newsletter

Follow us on