



// howden

bpif insurance services

Your defence toolkit

How to combat the cyber threat



Contents

The threat of cyber crime	4
How UK businesses are targeted	6
Recent cyber attacks	8
Why cyber security is so important to printers now	10
The General Data Protection Regulation (GDPR)	12
Protecting your print business	14
How cyber liability insurance can help you recover	15
How to buy the right cover for you	16
Howden's cyber expertise	18

The threat of cyber crime



Cyber crime is becoming an increasing threat to UK businesses - and the print industry is no exception.

The print industry has seen a number of cyber attacks in recent years.

Printers are often targeted because they hold large amounts of personal data. For example, many print firms are involved in the printing and mailing of credit card statements which is extremely valuable to criminals.

Furthermore, the use of cloud storage, online printers and 3D printers also opens print businesses up to exploitation.

46% of all businesses have identified at least one cyber security breach or attack in the last 12 months.*

***Source:** Cyber security breaches survey 2017, UK Government Department for Culture, Media and Sport in association with Ipsos MORI and the University of Portsmouth

How UK businesses are targeted



Whilst we all might think that we can spot a scam, hackers use various sophisticated ways of attacking businesses. Even large corporate businesses struggle to protect themselves from cyber crime which has resulted in numerous high profile cases in recent years.



Sophistication of attack	Typical victim	Technique
Low technical ability	Wide range of individuals and businesses	Financial Trojans - Malicious software that is sent via email as an attachment or web link. The attacker can then hijack and modify the victim's online banking transactions.
Low technical ability	Wide range of individuals and businesses	Commodity ransomware – Malware that blocks the victims from gaining access to their computer or mobile and then demands a ransom payment to restore.
High technical ability	High net worth individuals and businesses, normally targeted through their supply chains and customers	Repurposed banking Trojans – Hackers harvest and index victim data, installing remote access tools so they can access their victim's online devices and accounts.
High technical ability	Wide range of businesses	Business email compromise / CEO fraud – Hackers email payment clerks impersonating as the company CEO. They normally instruct the clerk to pay a sum of money into an unknown bank account.
High technical ability	High net worth individuals and businesses, normally targeted through their supply chains and customers	Targeted ransomware – Bespoke ransomware designed to target specific vulnerabilities of IT systems. E.g. the recent WannaCry incident which affected the NHS in May 2017.
High technical ability	Financial systems and infrastructure	Breaking into banks and financial systems – Hackers often target 'weak links' such as smaller banks or those in less developed countries.

Source: Closing the gap: Insuring your business against evolving cyber threats, Lloyds of London in association with KPMG and DAC Beachcroft

Recent cyber attacks



Case study 1

Scenario: A small UK print business was targeted with CEO fraud. The accounts clerk was sent an email that appeared to be from the managing director, instructing them to pay funds into two accounts.

Consequences: The accounts clerk transferred £20,000 into two legitimate UK bank accounts whilst the managing director was overseas. The attackers tried once again when the managing director had returned which was when their suspicions were raised.

Financial impact: The banks were unable to retrieve the money as the bank accounts had already been closed.

Insurance response: Business funds would be recoverable under the cyber insurance offering in line with sublimit purchased. Advice would also be available to prevent a repeat of such an event.

Case study 2

Scenario: A link was sent to an employee at a small company in the UK, malware was unintentionally downloaded onto the server and all data was encrypted. The attacker demanded £10,000 in Bitcoin for the decryption key.

Potential consequences: Loss of valuable data as well as a significant pay out, with no guarantee of regaining the data.

Response: The company phoned the incident response helpline provided as part of their cyber insurance policy. IT forensic investigators were brought in to analyse the breach and assess whether the ransom could be avoided and calculate the extent of loss.

Financial impact: The costs associated with response and data recovery totalled £60,000. Although this was more than the ransom, cyber insurers are better placed to advise in these circumstances. In most cases it is not recommended to pay cyber attackers; paying a ransom perpetuates criminal activity, there is no guarantee that you will regain the lost data and it is likely to encourage future attacks.

A 3D maze with glowing orange and yellow lines, symbolizing complexity and security. The maze is composed of many interconnected paths, creating a complex and challenging environment. The lighting is dramatic, with bright highlights on the edges of the maze and deep shadows in the recesses, giving it a sense of depth and mystery. The overall color palette is warm, with shades of orange, yellow, and red, contrasting with the cool blue and teal background.

Why cyber security
is so important to
printers now

Any business that holds customer data or uses a computer system within its business model needs to have robust cyber security and a tested contingency plan in place should things go wrong.

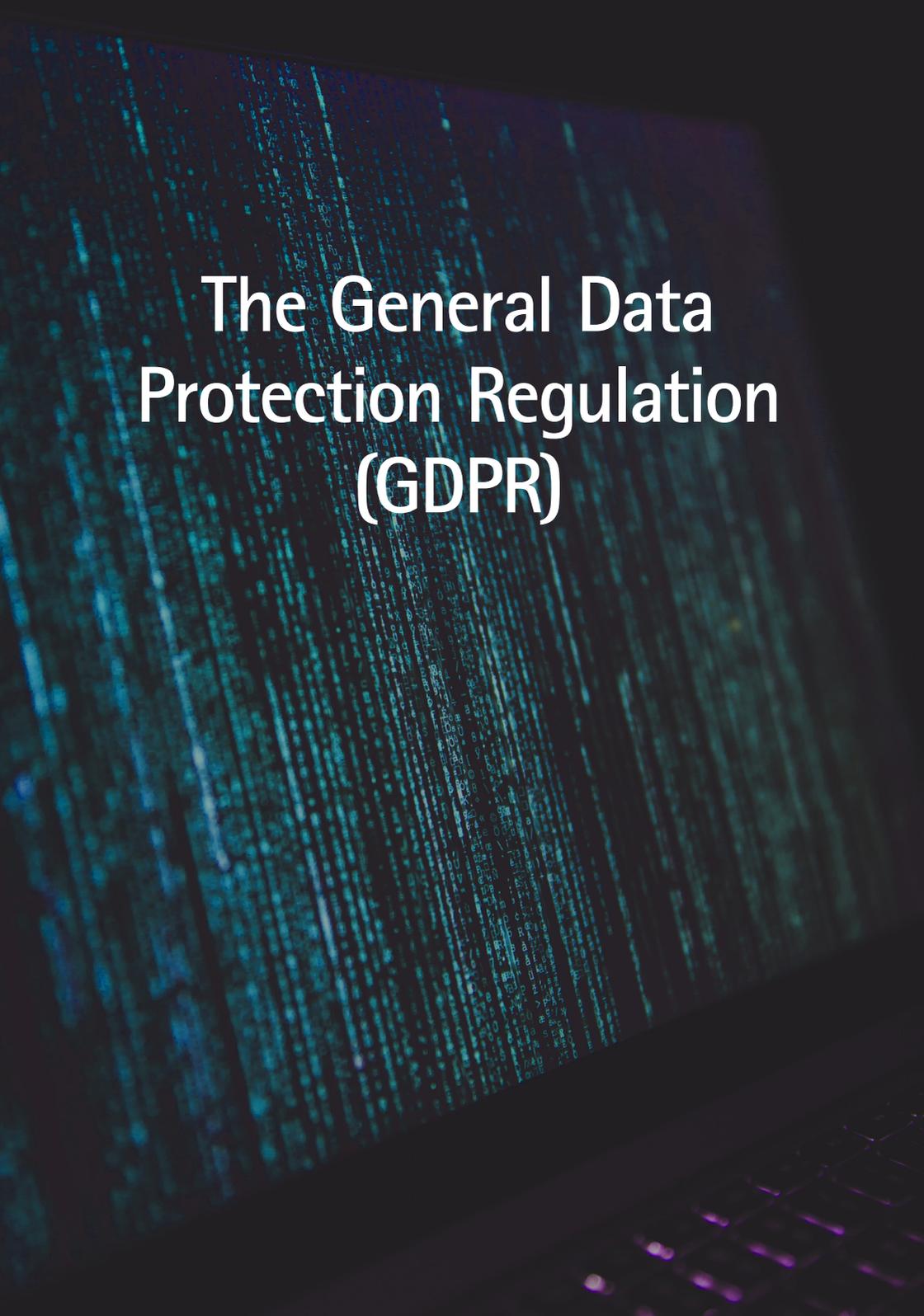
Potential immediate effects of a cyber attack

- Loss of access to files or networks
- Missed customer deadlines
- Software or systems corrupted or damaged
- Website or online services taken down or slowed
- Lost access to relied on third party services
- Permanent loss of files
- Money stolen or ransom charged
- Personal data altered, destroyed or taken
- Lost or stolen assets or intellectual property
- Machinery failure – unable to control lighting, heating or printers

Potential costs to your business

- New security measures needed to prevent future attacks
- Added costs of additional labour to deal with a breach or to notify clients
- Other repair or recovery costs
- Provision of goods and services interrupted
- Discouraged from carrying out intended future business activity
- Customer complaints/reputational damage
- Loss of revenue or share value
- Goodwill compensation to customers
- Fines or legal costs

Source: Cyber security breaches survey 2017, UK Government Department for Culture, Media and Sport in association with Ipsos MORI and the University of Portsmouth



The General Data Protection Regulation (GDPR)

After May 2018, businesses in the UK and Europe need to adhere to the new GDPR. Breach of these regulations could incur fines of up to 20 million euros or 4% of group worldwide turnover (whichever is greater).

Under the GDPR, businesses must have a lawful reason to hold and use personal data (such as consent, contractual necessity or legitimate interest), and demonstrate how data is securely processed.

Printers often hold large amounts of third-party data and, under the new regulations, are just as liable as the data owners. Therefore businesses need to ensure all information is secure and appropriately recorded and processed. Print businesses also store their own data, such as employee and recruitment information, which must also be included in the GDPR.

Businesses have to continually monitor for breaches of personal data and must notify the Information Commissioner's Office (ICO) within 72 hours of discovery.

Protecting your print business



There are four key pillars to an effective cyber defence strategy

The first step for many businesses is to have robust cyber defences in place. These should be arranged by experienced IT professionals and be appropriate for the size and nature of the business itself.

Thorough business continuity planning is important. Your business should consider how it would recover in the event of a cyber attack, for example, what would happen if the company servers could not be accessed?

Staff training and awareness exercises will help minimise the risk of a cyber attack. Do employees know how to recognise a cyber threat? Do they know how to manage the situation if an attacker is successful?

In the event of a cyber attack, cyber insurance can help reduce business interruption by covering the short term and long term costs involved, such as paying another supplier to fulfil customer orders and fronting ongoing legal fees.

How cyber insurance can help you recover

Cyber liability insurance provides support and financial cover to manage the immediate and long term impacts of a cyber attack.

- Incident Response (24/7 response line) to help you get back up and running as soon as possible
- Legal/Regulatory Costs, IT Security & Forensic Costs, Crisis Communication Costs & Privacy Breach Management Costs
- Third Party Privacy Breach Management Costs
- Remediation Costs/Mitigation Expenses
- Cyber Crime (sub-limited) – Funds Transfer Indemnification/Social Engineering, Extortion, Telephone Hacking, Phishing
- System Damage & Business Interruption (Consequential Reputational Harm)
- Network Security & Privacy Liability
- Media Liability (Defamation/IP Infringement)
- Court Attendance Costs

How to buy the right cover for you



The digital space is rapidly evolving, presenting new cyber threats all the time. Therefore, you should choose a specialist insurance broker who can save you time searching the market for the cyber liability product you need. Insurance brokers have access to many products and are regulated by the Financial Conduct Authority (FCA) so they offer advice you can trust.

A good broker will undertake a risk assessment and review of your current policies so you can determine your requirements and review any gaps in cover. They will also provide an impact analysis which will help with your business continuity planning.

For example, do you have the funds available if your business is charged a ransom? Does your IT team have the expertise to restore the network if corrupted or would you have to hire specialists? Would you need to hire a PR agency to manage the crisis communications?



Howden's cyber
expertise

Howden has strong expertise in providing cyber insurance solutions for a wide range of businesses.

- 45+ Insurers/Lloyd's Syndicates that Howden interact with offering variety and peace of mind to clients
- Volume Facilities
- Multi-layer transnational placements
- Strong insurer partnerships which allows us to negotiate the most appropriate deals for our clients
- Global expertise and network at the forefront of obtaining new coverages for clients

Howden and the BPIF

Howden provides BPIF insurance, specialist cover for businesses in the printing sector.

Howden has helped numerous BPIF members to achieve their commercial objectives, from reducing business risk with improved contributions from insurers to stabilising premiums to enable more accurate long-term budgeting.

Howden truly understand the nuances of the printing sector and recognise the benefits BPIF membership brings in terms of risk reduction.

If you would like more information or to discuss your cyber insurance requirements please contact us.

Howden UK Group Limited

16 Eastcheap, EC3M 1BD London United Kingdom

T +44 (0)20 7623 3806

F +44 (0)20 7623 3807

E info@howdengroup.com

www.howdengroup.co.uk

// Part of the Hyperion Insurance Group

Howden is a trading name of Howden UK Group Limited, part of the Hyperion Insurance Group. Howden UK Group Limited is authorised and regulated by the Financial Conduct Authority in respect of general insurance business. Registered in England and Wales under company registration number 725875. Registered Office: 16 Eastcheap, London EC3M 1BD. Calls may be monitored and recorded for quality assurance purposes. 02/18 Ref: M1671



Broker at **LLOYD'S**