Cyber-security Breaches Survey 2019

Presented by

Pound Gates

POUND GATES

CHARTERED INSURANCE BROKERS

Cyber-security:
A Rampant Risk Across Industry Lines

Regardless of industry, a wide range of factors have contributed to cyber-security taking the top spot on the list of common organisational risks this past year. Indeed, many sectors across the country have joined in the race to go digital as reliance on workplace technology continues to grow. In fact, 98 per cent of businesses and 95 per cent of charities depend on some form of digital communication and services (eg email, e-commerce or online banking) in the UK. As a result, the risks that come with technology implementation followed—over 30 per cent of businesses and over 20 per cent of charities reported that they have experienced a data breach or cyber-attack in the past 12 months. And those are just the attacks that we know about and that were reported to the government. What's more, the consequences of these attacks are significant—lost or stolen data, business interruption, financial concerns and reputational damage often accompany a data breach.

Fortunately, many organisations are taking steps to prevent the growing risk of cyber-attacks from wreaking havoc within their workplace. Nearly 80 per cent of businesses and 75 per cent of charities now rate cyber-security as a high priority in their organisation—significantly more than ever before. Such growth emphasises the importance of taking part in this rising effort to combat data breaches.

The Impact of the GDPR

As the GDPR celebrates its first anniversary, it's no secret that the implementation of this strict data privacy law is partially responsible for increased cyber-security efforts in the UK over the past 12 months. At a glance, 30 per cent of businesses and 36 per cent of charities reported making changes to their cyber-security programmes in the past year because of the GDPR. And while ensuring GPDR compliance might have felt like a tedious or unimportant task within your workplace, recent data found that GDPR-ready organisations experienced significant tangible benefits in response to their efforts—those that are compliant are 15 per cent less likely to suffer from a data breach. These numbers make it clear that GDPR-readiness is crucial now more than ever to reduce your risk of a cyber-attack.

With this data in mind, Pound Gates is proud to present our report summarising the 2019 Cyber Security Breaches Survey, commissioned by the Department for Digital, Culture, Media & Sport as part of the National Cyber Security Programme.

As you read through these numbers, consider what you can do to bolster your business' or charity's cyber-security practices and GDPR compliance efforts. Don't miss out on the expansive opportunities of selling online or resign your business to cyber-attacks because you failed to value cyber-security. Businesses can protect themselves and ensure online success with cyber-risk management guidance and insurance protecting against cyber risks, available from Pound Gates today.

INCIDENCE AND IMPACT OF BREACHES

This section summarises how many businesses and charities have experienced breaches throughout the past year, as well as the impact of those breaches.

Specifically, it visually quantifies how many organisations have experienced a breach, the most disruptive forms of breaches and the most common negative impacts that accompanied a breach.

Experience of Breaches

32% of businesses and **22%** of charities experienced a breach in the past 12 months.
Of these breaches:

32% of businesses and **29%** of charities needed new measures to prevent a future attack.

27% of businesses and **32%** of charities took up staff time dealing with the breach or attack.

19% of businesses and **21%** of charities had to stop staff from carrying out their daily work.

The Most Disruptive Breaches

Most disruptive forms of cyber-attack among organisations in the past 12 months:

Fraudulent emails or being directed to fraudulent websites (**49%** of businesses and **63%** of charities)

Others impersonating the organisation in emails or online (**15%** of businesses and **9%** of charities)

Viruses, spyware or malware (**9%** of businesses and **10%** of charities)

Impact of Breaches

30% of businesses and **21%** of charities that experienced a breach or attack reported suffering negative impacts, such as:

Temporary loss of access to files or networks	Websites or online services taken down or slowed	Software systems corrupted or damaged

DEALING WITH BREACHES

This section displays the numbers behind how organisations handled breaches in the past 12 months. Specifically, this section visually represents how long organisations took to identify and recover from a breach, the average cost of a disruptive data breach and action taken by organisations following a cyber-attack.

Time Taken to Identify a Breach

Average amount of time organisations took to identify their most disruptive breach or attack within the last 12 months:

62% of businesses detected the breach immediately, while **27%** did so in within 24 hours and **6%** did so within a week.

57% of charities detected the breach immediately, while **33%** did so within 24 hours and **5%** did so within a week.

Time Taken to Recover From Breaches

Average amount of time organisations spent dealing with their most disruptive breach with outcomes in the last 12 months:

Businesses overall: **3 days** Small businesses: **2.9 days** Large businesses: **3.1 days** Charities overall: **4.5 days**

Financial Cost of Breaches

Businesses overall:	Small businesses:	Large businesses:	Charities overall:
£4,180	**£3,650**	**£22,700**	**£9,470**

Understanding and Responding to a Breach

Only **16%** of businesses and **11%** of charities have a formal cyber-incident response plan.

44% of businesses and **48%** of charities don't know what factors led to their most disruptive data breach.

Only **24%** of businesses and **19%** of charities reported their most disruptive breach to at least one external body other than their cyber-security provider.

In response to experiencing a breach, **68%** of businesses and **71%** of charities are taking action to protect their organisation from future attacks.

APPROACHING CYBER-SECURITY

This section provides information on what actions organisations have taken to bolster their cyber-security efforts. At a glance, this section identifies common cyber-security controls and policies organisations implemented, staff training and awareness related to cyber-security, how many organisations have followed government cyber-security initiatives, average investments in cyber-security and cyber-insurance, and cyber-security documentation practices.

Cyber-security Controls and Policies

The top controls organisations have implemented to bolster their cyber-security include:

Applying software updates when available	Having up-to-date malware protection	Using firewalls with appropriate configuration

33% of businesses and **36%** of charities have a formal policy or policies covering cyber-security risks. Common features of cyber-security policies include:

- **What staff are permitted to do on the organisation's IT devices**
- **A document management system**
- **What can be stored on removable devices (eg USB sticks)**

Staff Training and Awareness

35% of businesses and **30%** of charities have at least one board member or trustee that is responsible for cyber-security.

27% of businesses and **29%** of charities reported training staff on cyber-security.

42% of businesses and **49%** of charities have staff whose job role includes information security or governance.

Understanding Government Initiatives

56% of businesses and **41%** of charities have implemented government initiatives related to cyber-security.

Investment in Cyber-security

70% of businesses and **40%** of charities had some level of spending on cyber-security in the past year.

Average investment in cyber-security in the last financial year:

- Businesses overall: **£5,100**
- Small businesses: **£3,490**
- Large businesses: **£277,000**
- Charities: **£1,500**

APPROACHING CYBER-SECURITY

Cyber-insurance

Only **11%** of businesses and **6%** of charities have a cyber-security insurance policy.

Documenting Cyber-security

62% of businesses and **60%** of charities have taken action to identify and document cyber-security risks in the past 12 months. Top actions include:

- **Business-as-usual health checks that occur regularly**
- **Risk assessments covering cyber-security risks**
- **Internal audits**

THE GDPR AND CYBER-SECURITY

This section offers a visual representation of how much GDPR-readiness benefited organisations in the realm of cyber-security. Specifically, the graphic includes how many organisations have made cyber-related changes in response to the GDPR, what those changes are and how these efforts have helped organisations prevent cyber-attacks and mitigate their losses.

Response to the GDPR

30% of businesses and **36%** of charities have made changes to cyber-security because of the GDPR. Common changes include:

- **Creating new policies**
- **Adding extra staff training or communications**
- **Changing firewall or system configurations**
- **Creating new contingency plans**

31% of businesses and **32%** of charities have completed a cyber-risk assessment in the past year, an increase of **7%** and **8%** respectively since last year.

Top Ways Organisations Benefited From Compliance

Source: Cisco

When compared to non-compliant organisations, GDPR-ready organisations have benefited from compliance efforts in the following ways:

Shorter sales delays

Fewer data breaches

And in the event of a breach:

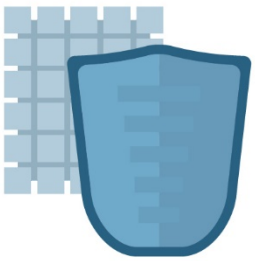
Fewer data records impacted

Decreased system downtime

Lower costs

THE IMPORTANCE OF CYBER-SECURITY

Top Reasons to Invest in Cyber-security



Protect customer and consumer data

Protect trade secrets, intellectual property or other assets

Prevent fraud or theft

Promote business continuity

Protect an organisation's reputation

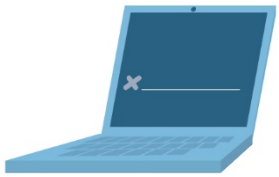
Comply with laws and regulations

Protect against viruses

INVESTING IN CYBER-INSURANCE

Why You Need Cyber-insurance

Government research suggests that cyber-insurance provides solutions for the following range of cyber-risks:



Privacy events

Network security liability

Cyber-crime

Network business interruption

Physical asset damage

Reputational damage