CYBER SECURITY FOR SMALL BUSINESSES

BREACHES, COSTS AND WHAT TO DO

University of Nottingham
UK | CHINA | MALAYSIA

Department for Digital, Culture, Media & Sport

Ipsos MORI

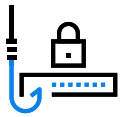
THE PROBLEM

The latest data from the government's Cyber Security Breaches Survey* shows that cyber incidents affect thousands of small businesses.

of micro and small businesses identified cyber security breaches or attacks in the last 12 months

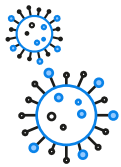
AMONG THIS 38%

Among the 38% identifying any breaches or attacks, there are a wide range of threats. Phishing is by far the most common, but impersonation and malware (including ransomware) are also significant issues.



82% identified phishing attacks

25% were impersonated online



13% identified malware (including ransomware)

27% were attacked at least once a week

22% needed new measures to stop future attacks

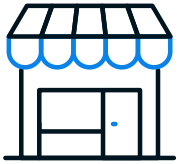
*Sourced from the Cyber Security Breaches Survey 2021 – full technical details and links to the source material are on the back cover of this booklet

THE SMALL BUSINESS VIEW

> If phishing incidents count then you would expect more like 100% of SMEs to experience a cyber incident.

> We had not really thought about the cost of a cyber breach.

> We have heard about cyber incidents in similar types of organisations to ours.



> How do we know if we're going over the top or not doing enough with security?

> An attack passed on from a large organisation could totally destroy our business.

> Many of the costs are hidden or not shared – people don't want to let others know.

Based upon participant feedback in small business workshop (February 2021)

THE IMPACT

The costs of cyber incidents can take many forms. They can be direct financial costs and indirect costs (e.g. your time). They can also continue to be felt over a long period. Knowing the costs will help you better prepare, with better decisions around how much to spend on cyber security, or how much time to invest in it.

Short-term direct costs

What was the value of any external payments made when the incident was being dealt with? This might include:

- Any payments to external IT consultants or contractors to investigate or fix the problem
- Any payments to the attackers, or money they stole

Short-term indirect costs

What was the cost of the staff time dealing with the incident (i.e. how much would staff have got paid for the time they spent investigating or fixing the problem)?

This still costs you – even if this was part of this staff member's job, they could have spent time doing other things.

Long-term direct costs

What was the value of any external payments made following an incident? For example:

- External payments to run audits, risk assessments or training
- The cost of new or upgraded software or systems
- Recruitment costs if you had to hire someone new
- Any resulting legal fees, insurance excess, fines, compensation or PR costs

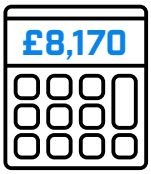
Other longer-term costs (including indirect ones)

What was the value of any damage or disruption during the incident? This might include:

- The cost of any time when staff could not do their jobs
- The value of lost files or intellectual property
- The cost of any devices or equipment that needed replacing

ARE YOU COMING OUT AHEAD?

- What are you spending on cyber security?
- Although it may not be specifically recorded as cyber security spending, some of your wider investment (e.g. IT spending) may be delivering safeguards and protection.
- What could a cyber security breach end up costing you?



is the average annual cost for micro and small businesses that lost data or assets after breaches*

*Sourced from the Cybersecurity Breaches Survey 2021

GETTING THE CORRECT BALANCE

- Cyber security may seem like a big ask if you are resource and time poor, but many basic steps are low-cost and not time-intensive
- Doing nothing is not a good option
- Knowing about the cost of breaches and the actions other small businesses take will help you avoid your own cyber security breaches
- Think about the costs you would like to avoid, and the safeguards that would support this

ALREADY READY?

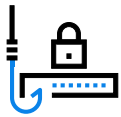
Three-quarters of micro and small businesses say that cyber security is a high priority for their directors (77%, vs. 69% in 2016).

But small businesses could do more to prepared themselves for a cyber incident.

Technical controls are important and most have these (e.g. 83% have up-to-date malware protection and 77% have network firewalls).

But good governance and staff awareness are also important and can often be improved.

33%
have done a cyber risk assessment



19%
have tested staff response
(e.g via mock phishing)

31%
have cyber security policies

13%
train staff on cyber security

WHO CARES IF YOU ARE CYBER SECURE?

Typically quite a number of people care about cyber security, including your customers, business partners, investors and others such as insurers.

There are also expectations resulting from regulations such as GDPR and possibly specific requirements in your sector.

WHAT DO YOU ALREADY UNDERSTAND ABOUT OUR OWN SECURITY POSITION AND POTENTIAL BREACH COSTS?

WHAT CAN YOU DO?

Cyber Aware

Cyber Aware is the government's advice campaign on how to stay secure online. It covers six essential actions that business owners and staff should take to make themselves cyber secure.

1. Use a strong and separate password for your email
2. Create strong passwords using 3 random words
3. Save your passwords in your browser
4. Turn on two-factor authentication (2FA)
5. Update your devices
6. Back up your data

Create your own free Cyber Action Plan in 3-5 minutes.

Cyber Security Small Business Guide

This guidance from the National Cyber Security Centre offers affordable, practical advice for businesses to improve cyber security. The guide covers five key steps:

1. Backing up your data
2. Protecting your organisation from malware
3. Keeping your smartphones (and tablets) safe
4. Using passwords to protect your data
5. Avoiding phishing attacks

You can also look at the guide for Response & Recovery from cyber incidents.

If you think you are ready to go further, you can see if you are ready for Cyber Essentials certification, using IASME's readiness tool.

ACKNOWLEDGEMENTS

The information in this booklet is drawn from the UK government's Cyber Security Breaches Survey 2021 and the 2020 report on Analysis of the full costs of cyber security breaches. It also includes findings from a cyber security workshop with small businesses conducted by University of Nottingham and Ipsos MORI in February 2021.

The material relating to Cyber Aware and Cyber Essentials is included with the permission of the National Cyber Security Centre.

- Survey findings reported in this booklet are taken from the DCMS Cyber Security Breaches Survey 2021.

Technical note on the Cyber Security Breaches Survey 2021:

- Ipsos MORI carried out a telephone survey of 1,006 micro and small businesses with 1 to 49 staff (excluding sole traders, and agriculture, forestry and fishing businesses) from 12 October 2020 to 22 January 2021. This included 380 micro and small businesses that identified a breach or attack in the last 12 months.

- The survey data are weighted to represent UK businesses by size and sector.

- See: www.gov.uk/government/statistics/cyber-security-breaches-survey-2021 for details of the full survey.

This booklet was produced for the
Cyber Security Group at the University of Nottingham.
www.nottingham.ac.uk/computerscience/research/cyber-security.aspx

University of Nottingham
UK | CHINA | MALAYSIA

Department for Digital, Culture, Media & Sport

Ipsos MORI