claranet

CYBERSECURITY TOOLKIT

Selecting the right policies, technology, and practices

Think of cybersecurity as a set of layers...

A **base layer**:	The firewall around your internal servers and internet gateways

Think of cybersecurity as a set of layers...

A **base layer**:	The firewall around your internal servers and internet gateways
A **second layer**:	How your resources are configured for access

Think of cybersecurity as a set of layers...

A **base layer**:	The firewall around your internal servers and internet gateways
A **second layer**:	How your resources are configured for access
A **third layer**:	Policies and controls on who can use your infrastructure

Think of cybersecurity as a set of layers...

A **base layer**:	The firewall around your internal servers and internet gateways
A **second layer**:	How your resources are configured for access
A **third layer**:	Policies and controls on who can use your infrastructure
A **fourth layer**:	Protection against inbound threats like malware and phishing attacks

Think of cybersecurity as a set of layers...

A **base layer**:	The firewall around your internal servers and internet gateways
A **second layer**:	How your resources are configured for access
A **third layer**:	Policies and controls on who can use your infrastructure
A **fourth layer**:	Protection against inbound threats like malware and phishing attacks
A **fifth layer**:	Patches and version control that keep your software up-to-date

Source: Cyber Essentials, National Cyber Security Centre

Then there’s a bigger level that over-arches the lot:

Then there's a bigger level that over-arches the lot: the way **human behaviour** can strengthen or compromise your IT security.

Power to the People?

It's a big issue. In SMEs, for example, it would appear **50%** of workers are using their own phones, tablets, laptops. Even more are using Shadow IT. (How many Dropboxes, Fileshares, webmail providers and social media apps are in use in your organisation?)

Yet when the network is breached... just 26% of companies report it to anyone outside their immediate circle.

Yet when the network is breached... just 26% of companies report it to anyone outside their immediate circle.

Sometimes because there's no policy to report a breach

Yet when the network is breached... just 26% of companies report it to anyone outside their immediate circle.

Sometimes because there's no policy to report a breach

Sometimes because there's no reporting pathway

Yet when the network is breached... just 26% of companies report it to anyone outside their immediate circle.

Sometimes because there's no policy to report a breach

Sometimes because there's no reporting pathway

Sometimes because of simple discomfort with sharing

Yet when the network is breached... just 26% of companies report it to anyone outside their immediate circle.

Sometimes because there's no policy to report a breach

Sometimes because there's no reporting pathway

Sometimes because of simple discomfort with sharing

Sometimes, from a fear that it might affect the share price.

This is despite the fact that

99%

of UK businesses are now using online services in some form.

The DCMS report says the costs are **SEVENFOLD**.

1

Making the investment

2

Insuring against threats

3

Training and education

4

Attaining good governance

The DCMS report says the costs are **SEVENFOLD**.

5

Managing the risk

6

Dealing with outsiders

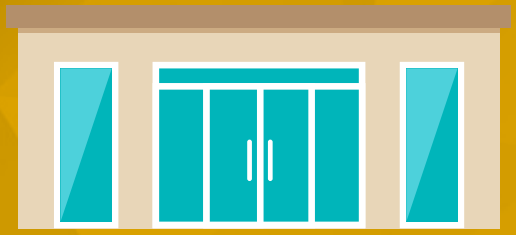
7

Reaching compliance

Investment in cybersecurity:

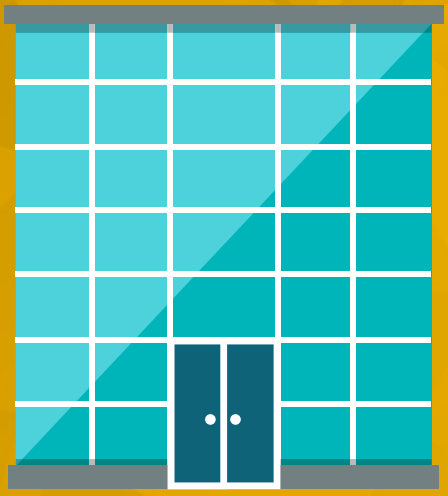
For small businesses it averages

£2,600



For medium-sized businesses it averages

£15,500



And for the enterprise it averages

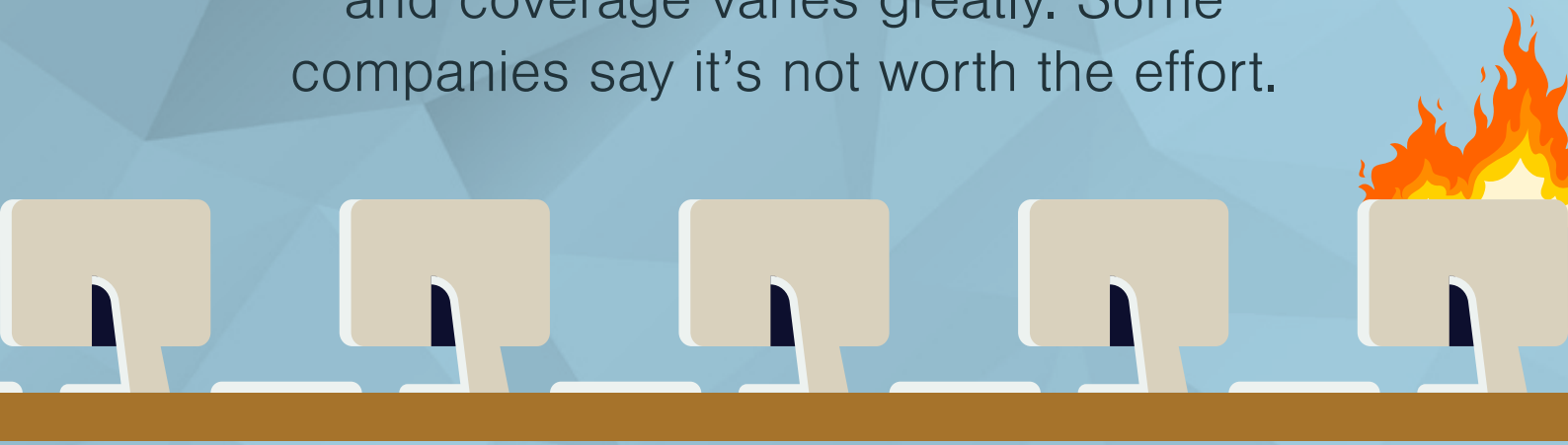
£387,000

Insuring against threats

38% of private companies took out formal insurance covering security breaches or attacks...

This rises to 57% in the education, health, and social care sectors.

But opinions on its value are mixed, and coverage varies greatly. Some companies say it's not worth the effort.



A policy that covers 10 PC's isn't much use in a company with 1,000 systems.

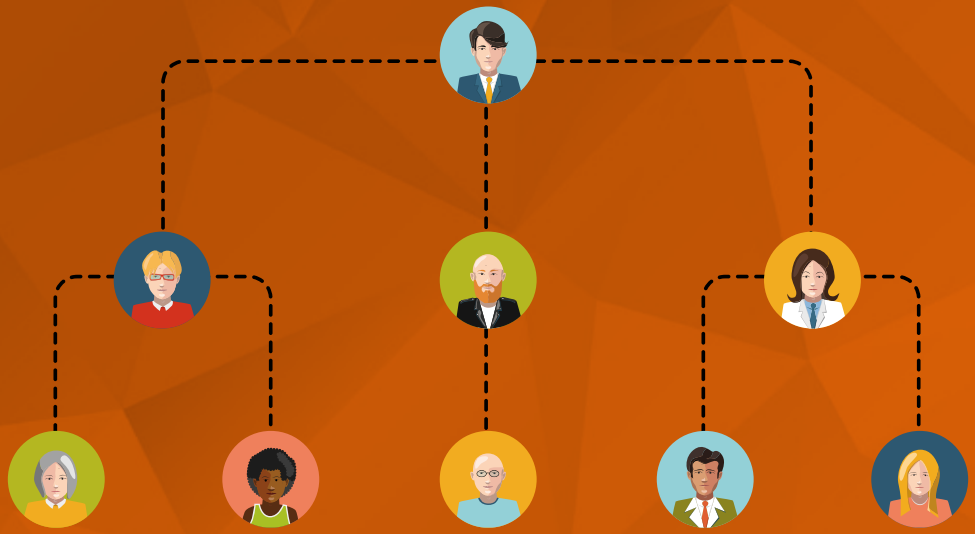
Training and education

IT security works best when **EVERYONE** has an understanding of how to handle sensitive data.

Educating employees is a key role of internal IT security staff, yet just

38%

of companies *even have* ITsec experts on payroll.



Attaining good governance

Few firms have made cybersecurity a board-level priority, with just **29%** naming a board member as responsible.

Yet assigning one leads to a clear increase in senior management attention to security issues.

Managing the risks

Good cybersecurity isn't about fixing things when they go wrong. It's about *pre-emption*.

57%

of all businesses have made progress with identifying risks in order to mitigate them.

57%

of all businesses have made progress with identifying risks in order to mitigate them.

9/10

have at least some rules and controls as formal policy.

57%

of all businesses have made progress with identifying risks in order to mitigate them.

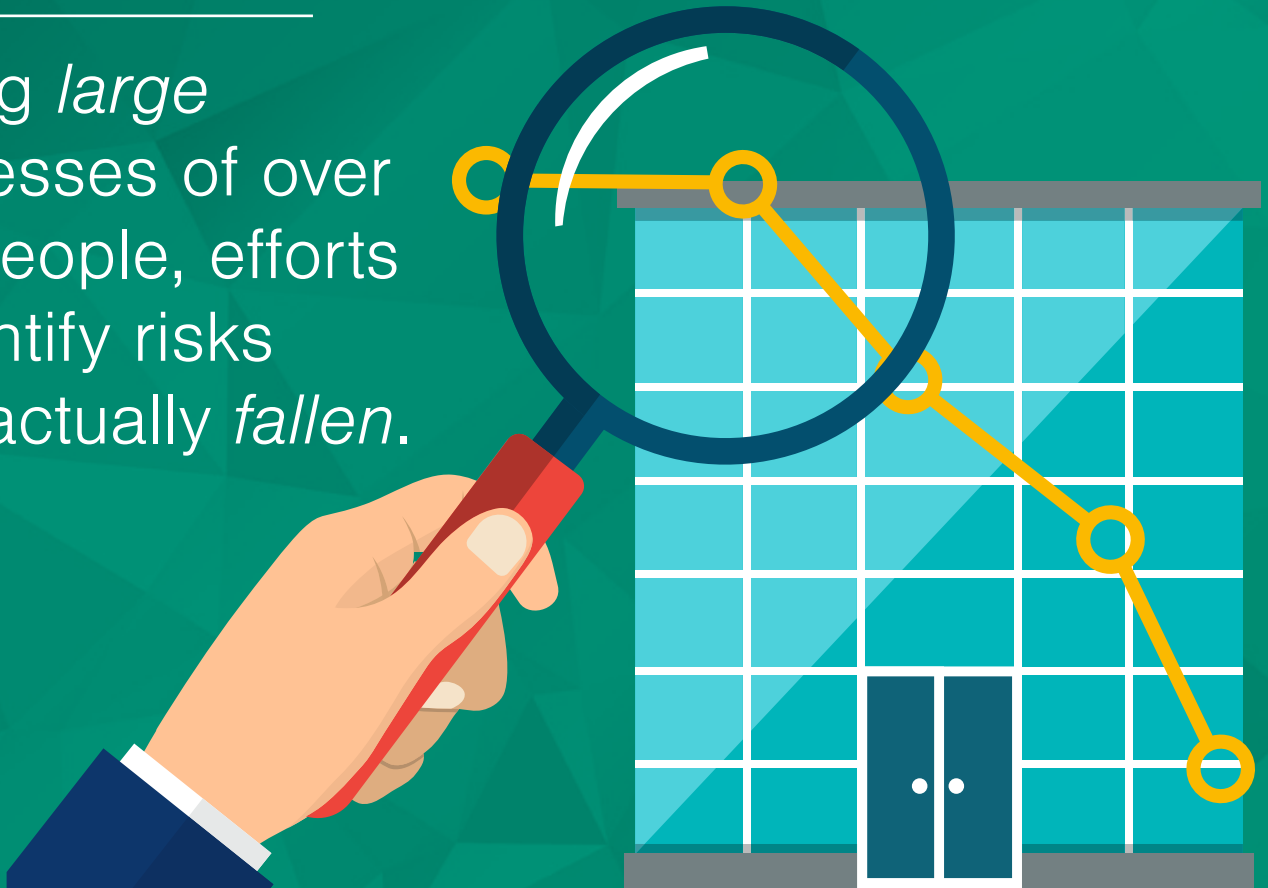
9/10

have at least some rules and controls as formal policy.

But far too often, personal and confidential customer data is still left unencrypted.

Key fact:

Among *large* businesses of over 250 people, efforts to identify risks have actually *fallen*.



Dealing with partners

In a connected world, security of your outsourced partners matters as much as your own.


Over half of companies say it's a concern.
Yet just
13%
require suppliers to agree to formal practices and processes.

Numerous “off the shelf” standards exist for suppliers to adhere to, including:

PCI DSS for payment cards

ISO 27001 for information security

The government’s Cyber Essentials framework

But only a few percent of companies have implemented them.

Reaching compliance

Programmes like Cyber Essentials aren't broadly known. Just **3%** of business recognise it.

But the good news is that many of these firms would meet these minimum standards as a result of existing policies anyway.

Cyber Essentials is a great first step, and isn't even that hard. Just a few days' consultancy can do it.

Cybersecurity may be a vast area.

But it can be tamed by being consistent about
POLICIES, TECHNOLOGIES, PRACTICES
... and getting everyone on-side.

KEY TAKEAWAYS

Focus management on the **business case** for cybersecurity.

The value created by keeping customer data safe.

The costs saved by an attack being avoided.

The resources freed for other tasks by automating processes.

The new customers out there when you reach compliance.


Good cybersecurity can
make your business more competitive.
Cybersecurity isn't a business **COST**... it's a business **OPPORTUNITY**.

To review the issues in hard numbers, take a look at our 2018 Research Report.

Download now

Beyond Digital Transformation:
Reality check for European IT and Digital Leaders

claranet
hosting | applications | networks

helping our customers
do amazing things