SKURIO

50 WAYS TO LOSE YOUR DATA

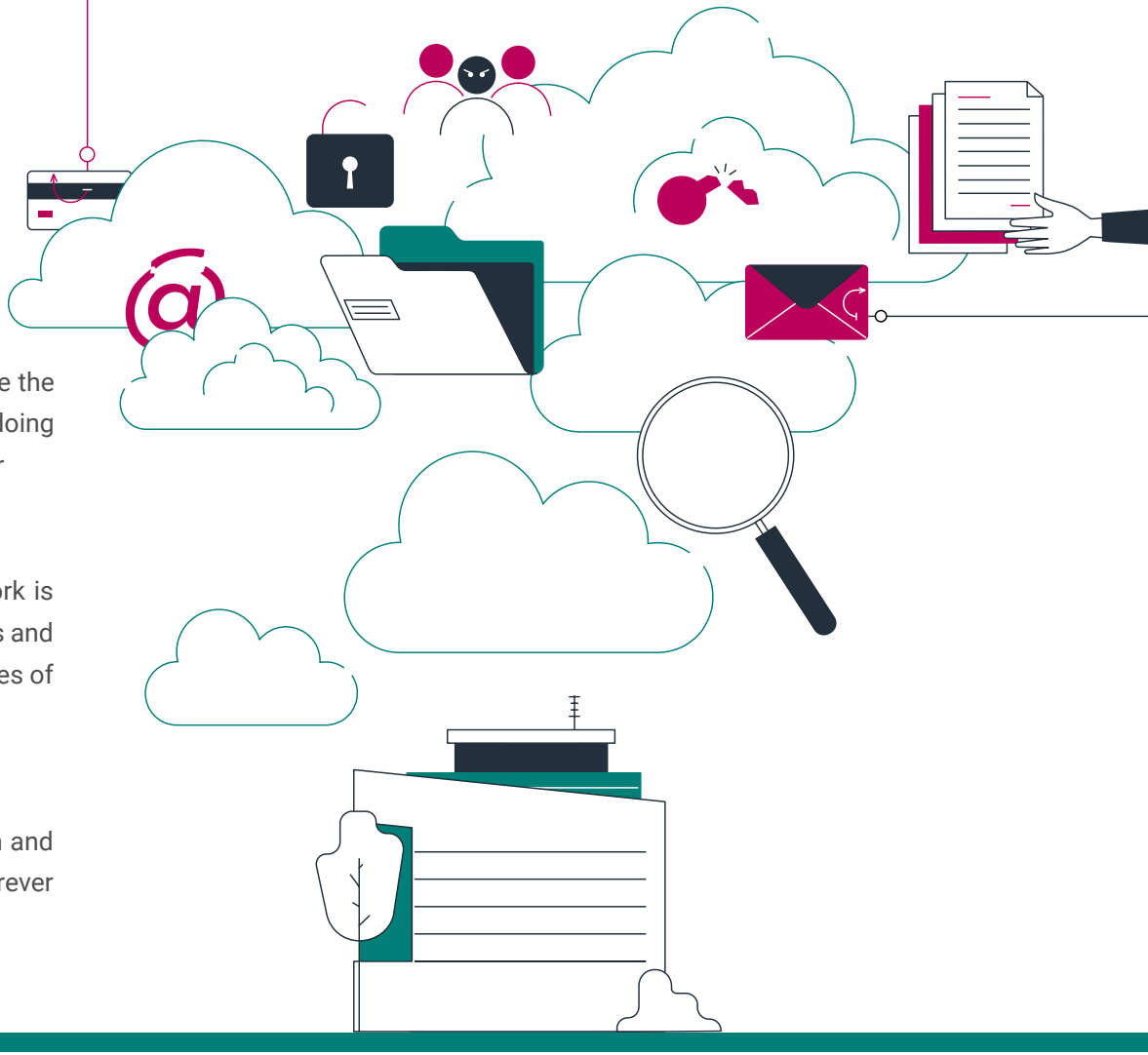
Understanding the true nature of data breaches

hello@skurio.com
www.skurio.com
+44 28 9082 6226

Table of Content

50 ways to lose your data

Your data has already left the building...



For decades the primary focus of IT security all over the world has been to secure the network. However, this 'inside the firewall' thinking ignores the obvious truth of doing business today: 'the network' now extends far beyond the firewall. Defending your corporate perimeter is no longer enough.

If you think about Cybersecurity from the point of view of your data, your network is just one of the places it lives. It also lives on the networks of your suppliers, clients and partners; on the Cloud services your business relies on; and on the portable devices of your employees. This diffusion of your data through your supply chain is a huge potential threat to your data security, a threat that is largely outside your control.

Accepting this fact means we need to update our approaches to data protection and Cybersecurity. We have to look outside the network and look after our data, wherever it lives.

Understanding the true nature of data breaches

When it comes to data breaches, the media's go–to image is of the lone hacker in a hoodie, hunched over their laptop in a darkened room, hacking into corporate networks and making off with the loot.

Clichés aside, hackers are undoubtedly a data security threat. Protecting your corporate network is still vital of course, you don't want to leave the front door open for anyone to come and go as they please.

But, in reality, bad guys breaking into your network and stealing the crown jewels represents only a small part of the picture. However, while virtually every business has bolted this front door securely, the back door is often wide open.

It's important here to stop and think for a moment about the huge variety of data your company holds: confidential client data; employee payroll data; customer passwords and payment card details; your own source code; marketing email databases. Now think about who has access to that data and where it is stored.

Much of it lives on your corporate network, but it is also legitimately shared with your clients and partners. It lives on the laptops your staff carry around with them. It's shared with payroll providers, HMRC, pension providers, and other service providers. Increasingly, large amounts live in the Cloud applications you use to run your business.

That's why bolting the front door to keep the bad guys out is no longer enough. There are a variety of other potential weak points which need to be considered, and you now rely on a lot of organisations outside of your control to have the same stringent levels of security as you do on your own network.

The reality is that all of these additional threat surfaces are probably more likely to be a source of a data breach than your own corporate network.

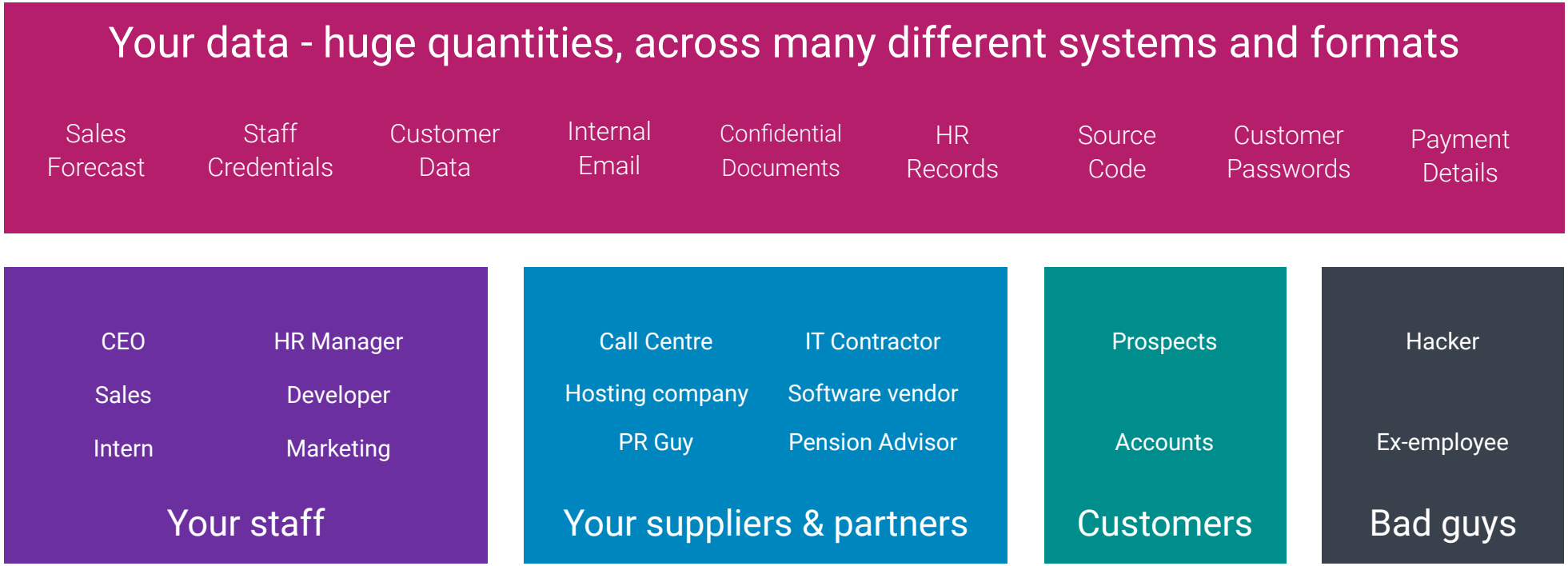


Figure 1 - Bad guys aren't wholly responsible for data breaches

So how does my data get out?

Slip out the back, Jack...

The short answer? Not necessarily how you think.

Ransomware incidents frequently make the headlines and there is an understandble misconception that most breaches are the result cyber attacks. The truth is much more mundane. Despite a steady expansion in the number and type of cyber attacks, most breaches are still accidential or down to human error. According to the ICO, a quarter of data breaches involving personally identifiable information (PII) in 2022 came from data being sent to an incorrect email address. Ransomware accounts for only 11% of breaches. See Figure 4.

Indeed, there are a host of scenarios that can lead to a breach that don't involve a malicious attack directly on your corporate network, such as:

- **Human factors:** data harvesting from a lost or stolen devices.
- **People doing their job:** a spreadsheet containing sensitive customer data shared with a partner or stored on a Cloud service.
- **Internal network security compromise:** employees clicking on phishing links or falling for social engineering attacks.
- **Third party breach:** where your data or your staff login credentials are accessed as a result of a Cloud app being hacked.

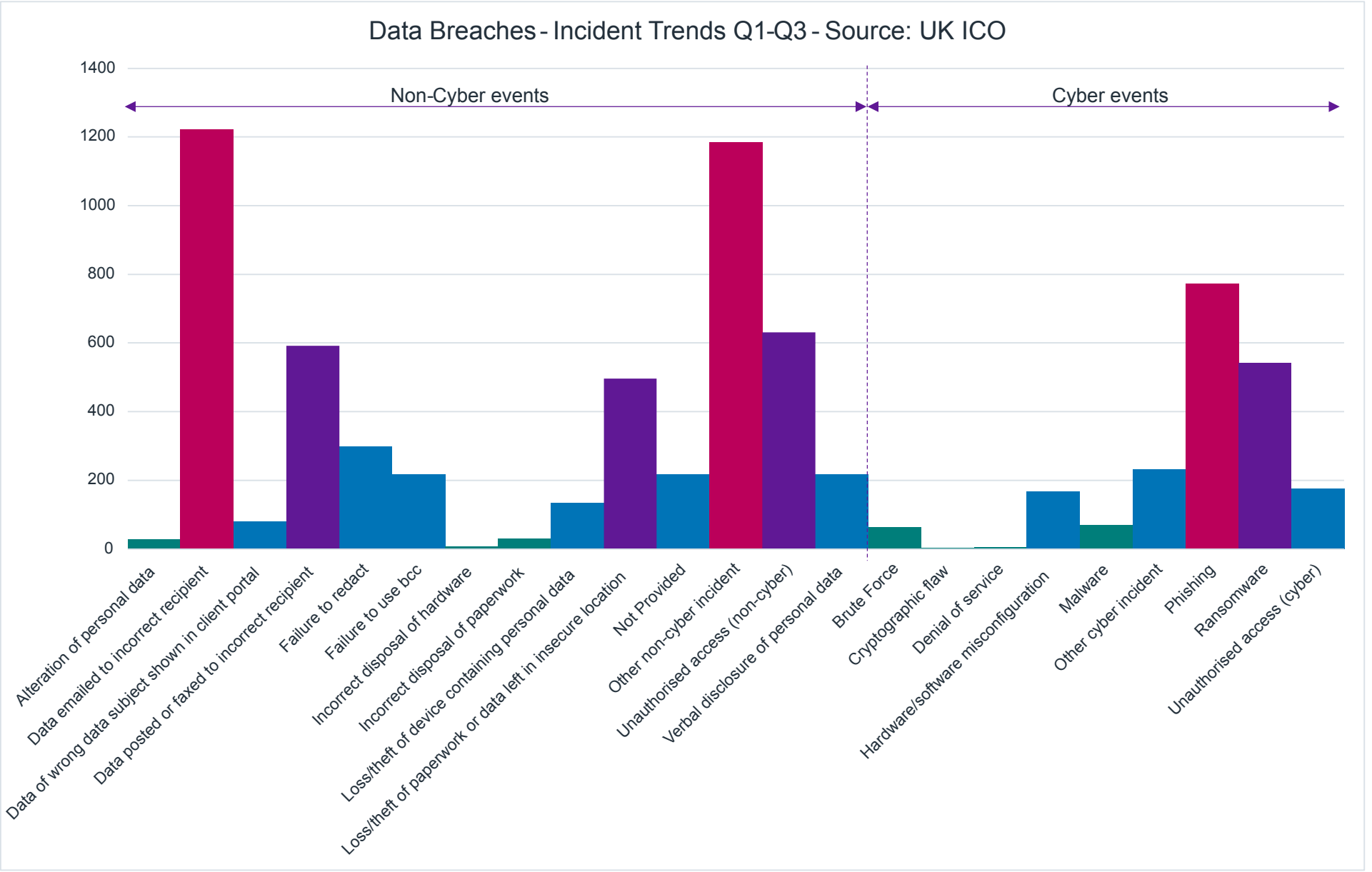


Figure 2 - Databreach disclosures and causes Q1-Q3 2022 Source UK ICO

It is inevitable that your company will suffer a breach caused by one of these incidents at some point. The important question is, where does your data end up once it's out?

If you're lucky your data will simply end up forgotten in an archive on a neglected server and never used. If the data includes email addresses it might end up on a relatively harmless spam list – a potential source of irritation to your employees and customers, but not a true security threat.

That's the best-case scenario. Equally your data could easily end up in the hands of your competitors or the media who may use your confidential information for their own advantage.

Figure 3 - Where your data ends up after a breach

Then there's the worst-case scenario – your data ends up on the Dark Web.

Whether acquired through malicious hacking or accidental breaches, criminals are after many different types of company data. These include export dumps from CRM systems, client information, employee login credentials, financial records, HR databases and more. However, like any business, cybercriminals need to market, distribute and sell their goods and the go-to place for this exchange is the Dark Web.

The Dark Web is the hidden part of the internet, not indexed by conventional search engines like Google or Bing. If you've heard of the Dark Web, it is likely as a network for illegal activities such as the sale of weapons and drugs. Cybercriminals now use it in exactly the same way to circumvent law enforcement to buy and sell corporate data. As specialists in Dark Web monitoring, we see hundreds, and sometimes thousands, of credentials and card details being shared or sold on the Dark Web every day.

What are criminals doing with this data? Most dangerously, they can use authentic login credentials to access your network completely undetected. They can also launch phishing and ransomware attacks on your company or your employees, or they can fraudulently use credit card details scraped from your data.

The consequences of criminals accessing your data in this way are obvious. There can be direct costs of paying ransoms, compliance fines (with GDPR, that could be up to €20 million or 4% of your global turnover), and the costs of repairing the holes in your network security. There are also the indirect impacts on your share price, customer confidence and negative PR, which are potentially more damaging.

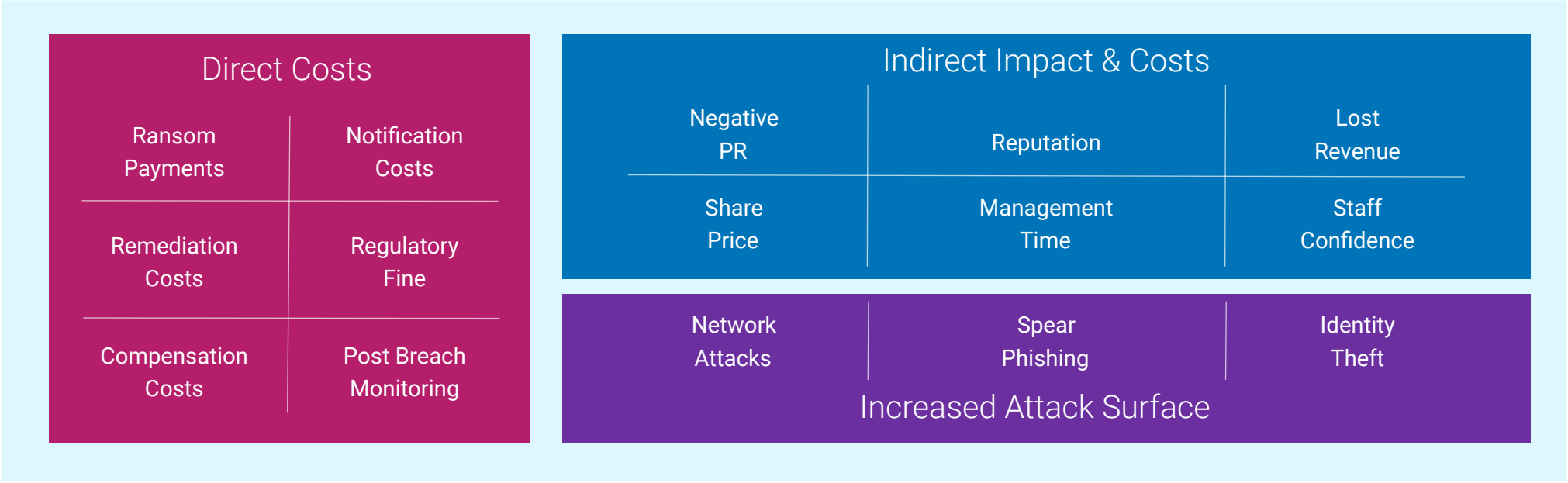


Figure 4 - The costs of breaches that happen 'outside the firewall'

There is also the risk if these attacks go undetected that you are increasing the potential for more, increasingly damaging, attacks to be launched in future. The longer you take to detect a breach, the more financial risk you face.

Ultimately, if you don't know where your data is, how can you hope to defend yourself properly?

What can I do about it?

Make a new plan, Stan...

Like most, you could add some new capabilities to your existing network security. Network log analysis or AI are great and can help to discover attacks and breaches. However, putting another bolt on the front door doesn't do anything about the back door that's still flapping in the wind.

What you really need is a tool that helps you keep track of your data by continuously looking outside your network perimeter for data appearing outside the firewall. This alerts you in real-time when your data is detected, so you can quickly take action to mitigate risk and minimise loss.

Skurio Digital Risk Protection continuously the surface, deep and Dark Web 24/7, then filters and extracts information based on your specific search terms, including (masked) email addresses, credit card numbers,
domain names, IP addresses and much more. When your data appears or is shared by cybercriminals, Skurio instantly alerts you.

As a fully Cloud hosted SaaS solution, Skurio requires no installation or connection to your network. You simply log in, configure your search terms (which can be as simple as one email domain, or thousands of keywords and IP addresses), and select how you would like Skurio to notify you of potential breaches.

Making your staff aware of credential breaches is quick and simple with a useful Teams integration. And, for more sophisticated users, Skurio APIs support integration with SIEM and IT service management platforms.

So...

There may be 50 ways to lose your data, but that doesn't mean you can't do something about it. It's time to look outside the firewall and make sure you're not the next company in the headlines!

SKURIO

Get In Touch

hello@skurio.com

www.skurio.com

+44 28 9082 6226