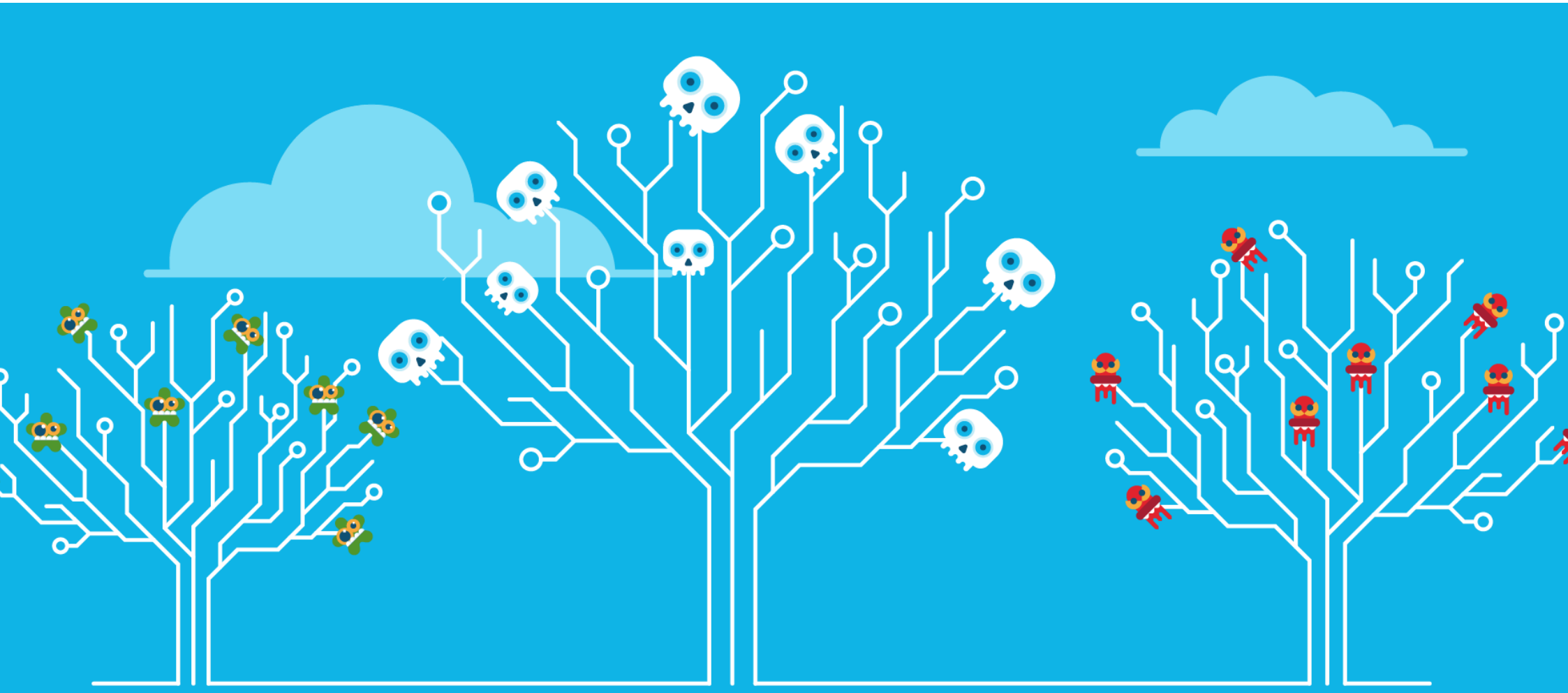

Threats are becoming more sophisticated

Hackers know your weaknesses and how to exploit them

Fewer of today's hackers are in it 'just for fun' or a challenge. Most are money motivated, highly organised and seldom work alone. Attackers are agile, while businesses can't always say the same. Especially when they've just been 'making do' with security.

'A hacker's goal is to steal credit card information, email addresses, usernames and passwords. Anything that can be sold on to a higher bidder. *How* they do it may include some of the following techniques.

Ransomware

Attackers can hold businesses virtually hostage, with ransomware; a ruthless practice. Ransomware remotely encrypts your files without your consent. Some forms of ransomware are programmed to spread across the network.

Instead of requiring a recipient to open an emailed attachment or click on a link, current trends in ransomware—such as WannaCry, which began in May 2017—enable malicious code to be transmitted between networks without user interaction. "WannaCry is the first one to completely automate," says Craig Williams, a senior security outreach manager at Talos, the security research arm of Cisco.

WannaCry affected more than 200,000 computers worldwide, and may cause an estimated $4 billion in losses. WannaCry gets installed through a vulnerability in the Microsoft SMB protocol and is particularly effective in older Windows environments, such as Windows XP, Windows Server 2003 and Windows 8. Microsoft had already released a security update to patch this vulnerability, but not all users were automatically protected.

Business Email Compromise (BEC)

Business email compromises (BEC) are 75% more profitable than ransomware. Despite that, they don't get as much publicity.

BEC are targeted attacks, in which hackers use social engineering to trick people into transferring money to them. There is no malware, there are no attachments. Unlike ransomware attacks, they don't take any data from their victims. It's all based on lies and misdirection.

Typically, hackers spend some time researching their targeted company and start building a profile. After they know enough, they may send spear phishing emails to senior members of staff, often in the finance department. It needs to be someone with the authority to transfer the money. The bigger the company, the more money they can make. However, attacks targeting small and medium-sized companies are on the increase.

The bigger the company, the more money they can make. However, attacks targeting small and medium-sized companies are on the increase.

Data Breach

Data is at the heart of everything your company does: it's your intellectual property, your next big break, your customer records, your revenue. A breach costs much more than just fixing outages and damaged systems.

Building a strong security posture can help protect your intellectual property and your reputation. On average, it takes organisations 191 days to detect a breach and 66 days to contain it. (Source: Ponemon Institute). Yet the key to damage limitation is early detection.

Too many businesses have a 'stacking problem'

Some businesses just don't have a clear cyber security strategy. They make do with a solution until it becomes a hindrance.

Others attempt to cover all bases and end up with a stacking problem. A stack of various point security solutions from different vendors, all in place at once. Both situations spell trouble.

The patchwork of incompatible security technology leaves gaps, creates management headaches and makes inefficiencies upon which hackers thrive. Each new security solution comes with another management interface. Each new solution demands human resources, management hours to set up, set policy, respond to alerts and it's not always clear whether the extra security outcome you gain is worth all the extra effort you are putting into managing that solution – rather than focusing on bigger problems elsewhere.

You may have added complexity without much overall incremental effectiveness. This situation isn't helped by the fact that security is still seen as primarily an 'IT issue'. According to the Cisco Security Benchmarks Study, some organisations don't particularly agree that line of business managers are engaged with security. The attitude is too often, 'Security is IT's problem.' This is a real issue, because it means that security often gets 'bolted on' rather than embedded in a company's ecosystem. Cutting corners creates more work.

Shadow IT

Shadow IT is the practice of employees using any applications they fancy, without getting the IT department's approval. This can be anything from installing an instant messenger service onto a work device, to downloading their own file sharing software and using it to transfer sensitive data.

Of the respondents participating in the Ponemon Institute's 2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB) report that experienced a data breach, 54 percent say negligent employees were the root cause—an increase from 48 percent of respondents in the previous year's study.

Shadow IT can create huge security vulnerabilities, especially if you don't know how far the problem extends. This kind of operation is like going for a swim in shark-infested waters wearing a meat suit. Yet it's incredibly prevalent in businesses. So why does it happen?

In fairness to staff, it happens with best intentions. Workers want to improve their own levels of productivity and use the latest digital tools. Staff are not usually thinking about the security implications when accessing these applications. Sometimes, employees use Shadow IT tools because they were used to certain systems in their previous organisation. After all, it's easier than learning something new.