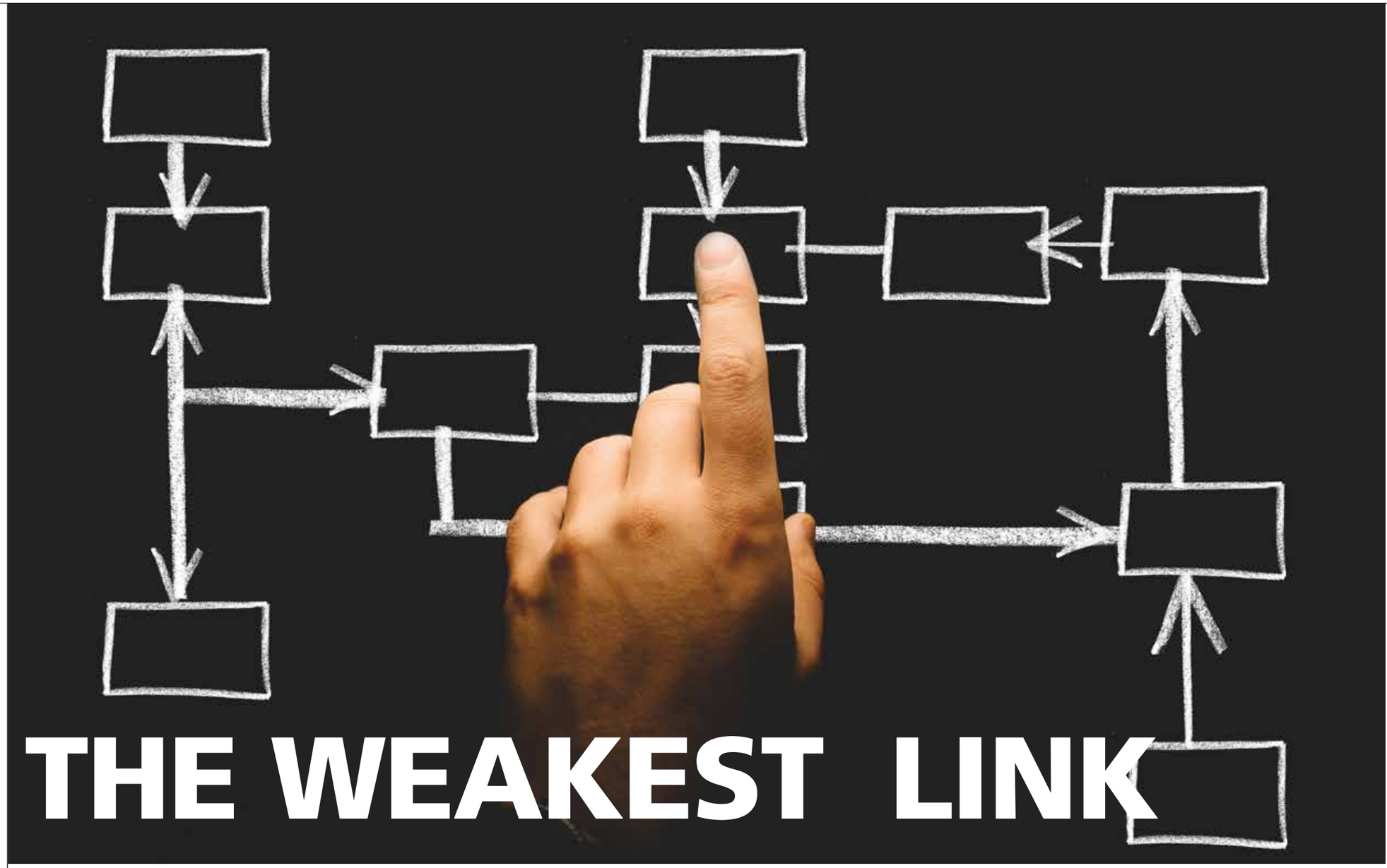

# THE WEAKEST LINK

**John Higginson** *explains why you need to start thinking about supply chain cyber security and looks at the growth of Business Email Compromise*

**Although your businesses will already have put in place measures to increase protection from growing cyber security risks, the next step is to think about your supply chain and whether the organisations that support you pose an acceptable risk or a weak link. Much like how you would be reticent to do business with an organisation with a bad financial credit rating, cyber supply chain risks should be seen in a similar light and it is important that you understand the threat to your business.**

There are two main ways in which the poor cyber security of your supply chain can have a direct impact on your organisation: if one of your suppliers is unable to provide you with the goods or services you rely on to operate your business due to them falling foul of a cyber attack, then this could potentially damage your output and reputation, particularly when bearing in mind just-in-time logistics or critical services. This is a risk you would want to avoid, or at the very least minimise and go with a supplier who has insulated themselves against cyber attacks. Secondly, your supply chain may be used as a backdoor to gain access to your network. You may ask why your supply chain should be any different from any other business, but the key difference here is that cyber criminals are the confidence tricksters of the 21st century and will look to exploit the trusted relationships you have with your supply chain.

**Identifying the weakest link in your organisation's supply chain is vital to a successful future**

Attackers can exploit this trust in different ways. Firstly, some of your suppliers may have access to your building management systems (heating, ventilation, power, lifts), which may be part of – or linked to – your network. If the supplier's network is compromised, yours might be too. A notorious example of this occurred in 2014, when the US retail business Target was hacked via its HVAC partner, losing credit card details of 110-million customers at a cost of $61-million.

Secondly, if your networks are not directly connected, this is another way in which trust can be exploited. The attacker can send spoof emails posing as the supplier, but with malicious content embedded to gain a foothold on your network. Due to the trusted relationship you have with this supplier, you are more likely to open any attachments to emails. Cyber criminals can go unnoticed on networks for long periods of time, utilising numerous approaches including monitoring traffic and patterns to establish the types of emails sent to partner organisations. By monitoring who the emails are from and what types of attachments are usual, this significantly contributes to their success.

## STAFF TRAINING SEEMS OBVIOUS, BUT ITS IMPORTANCE CANNOT BE UNDERESTIMATED

Having gained access to the environment, there are various ways in which an attacker can take advantage. It may be client details, such as bank accounts and email addresses, which can all be sold on the Dark Web. Alternatively, for a potentially bigger and quicker pay day they can conduct an attack known as Business Email Compromise (BEC). Increasingly prevalent and profitable, BEC works by the attacker monitoring the communications to understand how and when you invoice your clients. The attacker then sends an email from your finance department with your normal invoice, but critically then includes updated banking details for your clients to pay into. The attacker will delete any other invoices sent to the target client and cover their own tracks, usually by deleting what has been sent from your network. As the email comes from your network, your clients may well be duped into paying the invoice or indeed, you may get similar emails yourself. Although this attack may seem simplistic, it once again relies on the trusted relationships you have with both your supply chain and clients. Hugely successful, the FBI has estimated that $12-billion has been defrauded through BEC over the past five years.

To protect yourself from and in order to reduce your cyber security supply chain risks, here are some important things you need to consider:

Perform a baselining audit of who has access into your network and remove any unnecessary access, both from your staff and external suppliers, then continue to review regularly through an ongoing audit process.

Before taking on new suppliers or re-engaging existing ones, enquire about their cyber security maturity. While there is no industry standard questionnaire for supply chain assurance, the UK Government's Cyber Essentials+ would be a good place to start to show that they are at least thinking about it. Cyber Essentials identifies some fundamental technical security controls to help defend against internet-borne threats. The five controls are: Boundary Firewalls, Secure Configuration, Access Control, Malware Protection and Patch Management. There are cyber credit rating-type services available that can be helpful here too, but these shouldn't be viewed as a be-all-and-end-all solution. They can be useful comparatively, but in isolation can be also quite unhelpful.

Ensure you have robust processes in place in-house that do not allow any amended payments to be made without additional authentication, for example calling to confirm. Never call any numbers on an email that asks for a change in payment details – this is likely to be the attacker waiting for your call. Instead, call the known contact on a previously used number.

Educate your staff on what to look for and how to spot this type of attack. Staff training and awareness seems obvious, but cannot be underestimated in its importance. This means simple things such as making users change their passwords every few weeks, using a different password for each system and not clicking on suspicious links or attachments.

## DEFENCE IN DEPTH

Defence in depth is a term regularly used by the cyber security industry, but done well it is one aspect that can be added to improve supply chain vulnerabilities. The term simply refers to security being applied in multiple layers and works on the principle that each layer provides a different type of protection, providing the best chance of stopping an attack from getting through. Individually these layers offer some protection, but by using several there is better all-round coverage against multiple threats and no single point of failure.

The first layer is a firewall, which basically acts as a perimeter fence and makes sure only the right information can enter and leave a network. It won't stop every attack, but a well-configured firewall should be enough to keep the more opportunistic out. However, having one which allows employees to do their jobs thoroughly without letting any bad guy in can be tricky.

Another similar solution is an Intrusion Detection System (IDS). This essentially watches an IT system and identifies anything that doesn't look right. It's an early warning system and allows action to be taken as soon as something suspicious is detected.

Keeping logs is another layer. These can be generated for any and every action happening within a network and generate a large amount of data, which – although intimidating to anyone wanting to go through it and find something specific – is worth the effort as they can help identify incidents and aid a response. Logs can reveal a lot about suspicious behaviour, if something isn't working or if tighter control is needed. They can also work out how an attack happened and how to prevent another.

System hardening makes sure there is as little opportunity as possible for attackers to find an opening. This means going through and making sure unnecessary programmes are not running, all the latest updates are installed and access is locked down to only those that need it.

Finally, penetration testing can also form part of the layered approach and is highly effective in terms of identifying what gaps are present, are acted upon and then fixed before they can be exploited. Penetration testers simulate a malicious attack, from inside or outside of the organisation, in order to see how easy it is to break into a network or computer system and steal valuable data or deny access to critical assets. While penetration testing has traditionally been associated with government organisations and large financial institutions and corporations, it is now commonplace among medium-sized companies, NGOs and the wider public sector.

Remember, nothing and no one is infallible and determined attackers will continue for as long as it is profitable and works. It will no doubt evolve over time into something else, so you and your staff need to keep up with what is going on in order to be able to defend against it. Your organisation might not be the overall target, as you may be being used as a stepping stone to get to another more lucrative organisation – ultimately, we are all a part of someone's supply chain ●

**John Higginson** is Principal Consultant and Head of Incident Preparedness at Context Information Security and helps clients to understand and plan for cyber incidents, through the delivery and exercising at all levels and complexity of both incident response plans and technical playbooks.

**CIO John Mulligan testifies before the Senate Judiciary Committee after a substantial data breach at Target stores**

Picture credit: Getty