Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Ideally, brands and retailers will want to combine a robust fraud solution that can differentiate legitimate from fraudulent transactions across the buying journey with a flexible tool that can understand and monitor complex business policies. With the proper flexibility, a retailer can dictate under what circumstances extra steps should be taken to confirm that a human is doing the buying. And depending on the situation, the retailer can prescribe what extra steps are required – a Captcha or call to customer service, for instance. That sort of technology can ensure that an army of bots is not about to clean out the one product that everybody wants, but nobody will be able to get.

The good news is that the technology to help with scalping and rapid-fire fraud is available – and effective. The not-as-good news is that the scalpers and fraudsters are no doubt plotting their next work around as you read this. Rest assured, however, that the scalpers and fraudsters are not the only ones hard at work on the next new thing.

About the author
Gayathri Somanath is senior director of product at Signifyd, which provides fraud and consumer abuse protection for e-commerce. Somanath brings deep experience in e-commerce, payments and mobile apps to her work making commerce more profitable for merchants and more enjoyable for their customers. She has led Signifyd’s growth beyond guaranteed fraud protection and into areas focused on preventing consumer abuse resulting in illegitimate chargebacks and unauthorized reselling. She has a bachelor’s in computer engineering from Amrita University, Coimbatore, and an MBA from the University of California, Berkeley, Haas School of Business.

References
1. Mello, John. ‘Scalper bots hoarding hottest products from consumers’. Commerce Times, 9 Dec 2020. Accessed Mar 2021. www.ecommercetimes.com/story/86945.html.
2. Gilbert, Ben. ‘One reseller group snagged nearly 3,500 PlayStation 5 consoles, and the resale market might be the only place to score one after it sold out everywhere online’. Business Insider, 21 Nov 2020. Accessed Mar 2021. www.businessinsider.com/playstation-5-launch-day-us-europe-flooded-by-reseller-bots-2020-11?r=US&IR=T.
3. Molloy, David. ‘Christmas shopping: Why bots will beat you to in-demand gifts’. BBC News, 26 Nov 2020. Accessed Mar 2021. www.bbc.com/news/technology-55074383.
4. ‘AI vs AI’. Sync NI, 8 Nov 2019. Accessed Mar 2021. https://syncni.com/article/3261/ai-vs-ai.
5. Ridley, Jacob. ‘UK politicians call for making the resale of goods purchased using an automated bot an illegal activity’. PC Gamer, 15 Dec 2020. Accessed Mar 2021. www.pcgamer.com/uk/uk-parliament-reseller-bots/.

Defending against insider threats with network security’s eighth layer
Phil Chapman, Firebrand Training

It would be an understatement to say 2020 was a year of change, but here we are in March 2021, a world away from March 2020. As the UK Government juggles the socio-economic impacts of Covid-19 and now Brexit, daily news briefings are announcing new guidelines and initiatives to tackle a whole host of problems old and new yet it feels like the growing cyber security threat has been pushed to the bottom of the importance list.

Cyber security, unfortunately, can often be overlooked. A driver for this is a lack of understanding of the cyberthreat from some senior leaders, meaning that fortifying the organisation is seen as a drain on the bottom line rather than a company-wide problem. This lack of understanding has proven costly in the wake of the pandemic.

Almost overnight, much of the entire global workforce found itself setting up offices from bedrooms, kitchen tables or any other quiet spare corner in the home. This adjustment not only impacted staff but the entire business as tools and systems to enable efficient home working had to be rapidly implemented. This rush to adapt also brought up a massive problem – without the security perimeter of the office, how would private networks and the sensitive data within them be protected?

IT and security teams found themselves stripping back to the basics of network security to implement new structures and guidelines to protect against the threats that en masse remote working poses. The ‘insider threat’, which, of course, existed before the pandemic, suddenly became much harder to manage as staff were set loose to work...
on unsecured networks, on unsecured devices, while teams scrabbled to implement an ‘eighth layer’ to their network security strategies to quickly protect the organisation against this plethora of vulnerabilities. Exacerbating this further was the cyberthreat itself, which quickly shifted to capitalise on the opportunities that remote working opens up for attackers to infiltrate the business.

This article will look closely at network security, discussing its traditional definition as a seven-layer strategy as well as how it is currently being used, examining the impacts of the pandemic in particular and taking a closer look at the evolving threat. We will then focus on the so-called eighth layer of network security, look at why this is crucial in fighting against the growing insider threat and the ways that this layer can be implemented into existing security strategies.

**Defining network security**

Summarising network security to the readers of this publication may seem redundant, but to fully understand the current situation, let’s take a quick step back to review its development and different layers.

“*The tools and techniques utilised in the practice of network security fortify both the network and its infrastructure, deploying policy, software and even sometimes hardware to protect against cyberthreats*”

Every organisation, regardless of its size or industry requires a form of network security to protect itself. As we all know, this means that in its simplest terms a network is two or more computer systems connected by physical or wireless connections – so even a one-person business that uses just a laptop and a phone to operate needs network security. The tools and techniques utilised in the practice of network security therefore fortify both the network and its infrastructure, deploying policy, software and even sometimes hardware to protect against cyberthreats such as trojans, malware, adware and distributed denial of service attacks (DDoS), to name a few.

The concept of network security, alongside cyber security as a broader discipline, came into existence in the late 1970s and 80s. It then became more mainstream with the dotcom bubble of the 1990s and early 2000s. This is because after we welcomed the World Wide Web into our lives its uptake was sudden and rapid, making it hard to imagine a time before global connectivity. But with the good comes the bad, and with the Internet came a rapid evolution of the crime that exploited it – cybercrime.

**Complex construct**

From its early days, modern network security has evolved from a simple concept to a complex construct which operates in an ever-changing threat environment of cyber criminals looking for the weakest link. These weak links are present in many different areas, from applications and data to devices and locations, and if found can cause widespread disruption and damage to an organisation. For this reason, network security is built from many different layers designed to protect a network from external threats. These layers can be broken down in many different ways but one of the simplest is to split it into the seven different layers of the Open Systems Interconnection (OSI) model, or use the four-layer condensed TCP/IP model for reference. The first three layers – Application (receiving information directly from users and displaying incoming data to a user), Presentation (presenting data for the network) and Session (helping two devices to ‘speak’ to each other), which are known collectively as the Application layer – include protocols such as HTTP and DNS, which allow a device to connect to websites. The next is the Transport layer which allows two endpoints to connect securely or non-securely; then the Network layer (OSI) or Internet layer (TCP/IP) which allows for data to be addressed and routed correctly across networks; and finally the Data Link and Physical layers (OSI) or Network Access layer (TCP/IP) which allows for data to be physically prepared and then transmitted and received.

When creating a company’s network security, teams tend to follow this seven-layered approach to protecting a network. But there is an all-important eighth layer, ‘Layer 8’ is a term lovingly used by some service desks and IT technicians to refer to the users of the network or system. Ensuring that the organisation’s people are adequately educated in cyber-skills means they are working safely rather than creating vulnerabilities, and this layer is
now more vital than ever in maintaining the other seven layers.

Evolving network security
Traditionally, businesses build their network security infrastructure on site, allowing them to have more hands-on access to physical hardware (such as laptops, PCs and on-premise storage) and manage internal security policies (ie, don’t plug random USB devices into your computer’s ports). However, as we all know, the shift to remote working has fundamentally altered how organisations are able to manage their network security.

“In the blink of an eye, offices were deserted and the on-premise firewall that glued together these vital layers of network security became largely redundant, making organisations incredibly vulnerable to attack”

The layers of network security apply a multitude of security controls to weed out threats against the network. Depending on the layer in question, these measures range from access control, identification and encryption to URL filtering, authentication and malware detection, and are built through the deployment of firewalls, proxies and gateway management systems – the first technical line of defence of network security. When in the office, most businesses had an on-premise firewall in place that was key to securing every device connected to the on-premise network within an office. However, in the blink of an eye, offices were deserted and the on-premise firewall that glued together these vital layers of network security became largely redundant, making organisations incredibly vulnerable to attack. And cyber criminals took note.

Network security therefore had to adapt and change to fit this new future of increased remote working, with firewalls and additional layers of security having to be redesigned and adjusted to accommodate. However, in the rush to implement new technical solutions, teams must not forget the importance of protecting against the insider threat. In fact, even if this eighth layer existed in the business before Covid-19, a lot of time must now be spent to ensure it is fit for purpose in the face of this evolved ecosystem. In short, an organisation’s security relies to a large extent on the actions of its staff and no number of firewalls can protect against a lack of cyber security knowledge.

The threat landscape
The term ‘insider threat’ has two main variants. Firstly, people within the organisation that want to attack it or leak its data for criminal purposes. Secondly, which is much more common and exists within every single organisation in some form, is employees who lack cyber awareness or have limited skills will unwittingly take actions that put the business at risk. Throughout this article we have referred to the fact that cyber criminals have adapted to take

Average costs for the most disruptive breaches. Source: Nexor.

| Layer         | 2020      | 2019      | 2018      | 2017      |
|---------------|-----------|-----------|-----------|-----------|
| Long-term cost| £1,690    | £1,220    | £830      | £776      |
| Recovery cost | £1,830    | £1,830    | £847      | £937      |
| Direct cost   | £3,650    | £2,350    | £1,380    | £1,380    |

Types of cyber attack causing the most concern over the next 12 months. Source: Crowdstrike.

- Ransomware: 54%
- General malware: 53%
- Phishing/spear-phishing: 52%
- Password attacks: 43%
- Advanced targeted attacks: 37%
- IoT attacks: 37%
advantage of the fact that the insider threat is more prevalent than ever now that employees are working from home (WFH). This shift has created a vulnerability minefield, with staff linking devices to the company intranet, using home networks that likely have 12345 as a password, falling for increasingly sophisticated phishing emails and even leaving devices within arms length of family members who may not be authorised to see sensitive data.

“CybSafe claimed that 32% of organisations surveyed had experienced a cyber attack as a direct result of an employee working outside of the businesses’ security perimeter”

In addition, we have referred to how the cyber security threat landscape has evolved to take advantage of the pandemic, including the shift to working from home. This means that an important part of a security team’s job is to understand exactly what that threat is, and since this changes on a daily basis it can be very challenging to keep up. So we’ll summarise the key trends you need to know. This will showcase how the eighth layer comes into its own when we evaluate 2020’s threat landscape and look ahead at what we can expect from 2021.

Unrivalled year

There’s no doubt that 2020 was an unrivalled year for cyber attacks. The pandemic generated the perfect conditions for cyber criminals, with attacks rising by 31% in May – June 2020. The UK’s National Cyber Security Centre (NCSC) reported that over the past year it dealt with 194 coronavirus-related incidents involving criminal gangs, which led to the overall number of serious hacker attacks on the likes of the NHS, vaccine research departments and even supermarkets, reaching an all-time record of 723.

This drastic rise in the number of attacks has had damaging financial and reputational implications for the organisations at the receiving end, which, sadly for those already struggling due to the pandemic, could spell the final nail in the coffin. The numbers tell the story best, as according to a recent report UK businesses lost over £6.2bn to cyber scams from September 2019 to September 2020 with 3,445 businesses falling victim to attacks in the same period – 1,740 of those attacks (51%) took place during the UK’s first lockdown alone.

Many of these cyber attacks see criminals seek to exploit employees specifically, showcasing again the importance of having a robust eight-layer network security strategy. In 2018 CybSafe claimed that 32% of organisations surveyed had experienced a cyber attack as a direct result of an employee working outside of the businesses’ security perimeter. It would be no stretch to say that this will undoubtedly have increased with the shift to remote working. In fact, the Department for Digital, Culture, Media and Sport’s ‘Cyber Security Breaches Survey 2020’ found that businesses reported that the top reasons they went on to suffer a breach or attack (86%) was fraudulent emails or employees being directed to fraudulent websites. The second most-prevalent reason was that employees fell for cyber criminals impersonating the organisation itself in emails or online (26%).

Medium to large businesses have also identified unauthorised use of computers or networks by staff (21%) as a frequent reason for a breach: for example employees downloading apps or files for personal use on a work device. However, worryingly, in the same government report, 33% of businesses who reported a breach took no further action to prevent further incidents.

Sophisticated attacks

Employees have been vulnerable to different types of sophisticated attacks during the pandemic. One example was a targeted attack against Microsoft users, with cyber criminals looking to steal Office 365 usernames and passwords through a series of phishing emails using Captchas (asking people to check a box or identify a particular image) as a way of lulling victims into a false sense of security. This attack targeted a wide variety of businesses, from hospitality to finance and was successful in tricking employees into revealing passwords and usernames.

Another example is the rise of fake email attachments including ransomware, which remains one of the biggest security problems facing many organisations today. As criminals get better at impersonating...

Percentage of organisations that take the stipulated actions, or have these measures in place, for when they experience a cyber security incident. Source: Department for Digital, Culture, Media and Sport.
the business, employees are falling victim to these types of emails more and more, opening the harmful fake attachments that can lead to an attack on a single device or an entire network. Once this malicious software is opened it encrypts files and documents and is often only removed if demands for payment are met, costing the organisation vital resources.

As we head further into 2021 and remain in a world of ever-lengthening lockdowns and working from home, the cyberthreats of the past year look set to evolve at a similar pace. On top of this, the UK’s recent exit from the European Union has left many questions unanswered on the future of the UK’s cyber security. A particular concern centres around the need to recruit new digital talent into the UK, with 45% of businesses noting that a reduction in available talent will worsen the increased cyber security risk.7

The eighth layer

We’ve established that the insider threat is one of, if not the biggest threat to an organisation’s network security. But how can this risk be reduced in an ongoing WFH world and how can businesses safeguard themselves in the long run when a flexible approach to working is set to become the norm?

The all-important eighth layer needs to become intertwined into the building of a strong network security strategy and a large part of this centres around frequent and consumable dedicated training and policy updates. Troublingly, however, a recent report found that only 6% of businesses say they are ‘open’ to investing in cyber security training.8 It is paramount to a business that it becomes second nature to staff to not click on links in phishing emails, open attachments from unknown senders or use weak passwords. These might seem like obvious pitfalls to avoid but employees outside of the IT and security teams need continuous cyber security training to keep this learning top of mind in order to protect themselves and therefore the company from these ever-evolving threats. Just like breaking any bad habit, educating staff and continually emphasising individual responsibility will go far in reducing risk.

Alongside regular training, a business must also implement strict network security policies. Having a policy document in place will lay down standard protocols for all employees to follow, whether they are office-based or remote and working on a private network. This policy should clearly lay out the guidelines for computer network access and define security policies and procedures, informing staff and network users about the requirements for protecting corporate resources and underlining the risks involved if the guidelines are not followed. A carrot-and-stick approach works well: staff can be rewarded for completing training or flagging if a phishing email pops into their inbox, but equally there must be consequences if they are caught flouting the rules or continuously falling for attacks.

Businesses must start valuing all eight layers of network security and the role that the entire organisation plays in top-quality network security strategies. Everything must be done to help staff to not be the weakest link, with more investment directed to regularly upskilling and training staff before a breach takes place, not afterwards. After the past year, it has become apparent that companies can no longer dismiss network security as an isolated security or IT issue and to continue to not prioritise it could, in our current climate, spell the end of the business.

About the author

Phil Chapman is a senior cyber security instructor for Firebrand Training (https://firebrand.training/uk) who predominantly helps train UK law enforcement and cyber security apprentices. He has 24 years of military intelligence experience and 14 years of training/consultancy in infrastructure, networking and security.

References

1. ‘Why cyber security is more important now than ever’, Nexor, May 2020. Accessed Jan 2021. www.nexor.com/resources/reports/why-cyber-security-is-more-important-now-than-ever/.
2. Sabbagh, Dan. ‘Covid-related cybercrime drives attacks on UK to record number’. The Guardian, 3 Nov 2020. Accessed Jan 2021. www.theguardian.com/technology/2020/nov/03/covid-related-cybercrime-drives-attacks-on-uk-to-record-number.
3. Jones, Connor. ‘A third of cyber attacks exploit unsecure remote working’. ITPro, 20 Dec 2018. Accessed Mar 2020. www.itpro.com.
In a way, we hold these truths to be self-evident, that the cyber security field is populated and advanced by students of science, technology, engineering, and mathematics (STEM). However, this is not the whole truth, but rather a misconception fueled by hasty pop-cultural perceptions of the technology industry. The preconceived notion that only students of the hard sciences can contribute to the vast technology industry may actually prove to be detrimental to companies seeking very qualified and broadly experienced talent, simply by discouraging prospective professionals from even considering a cyber security career path because of their formal training and background in other, more liberal arts disciplines. Let’s look into this further.

**Crossing the cyber skills gap**

These negative stereotypes are not just perpetuated by pop-culture. They are often reinforced by high school guidance counsellors, who warn students going off to college that they will ‘never get a real job’ without a degree in the STEM field, thereby steering them away from the ‘softer’ subjects of the liberal arts and humanities fields.

In reality, despite this ‘encouragement’ of propelling students into the technological fields of study, many employers in cyber security still find a huge skills gap in many of their recruits coming from STEM fields. This all-or-nothing attitude toward STEM degrees and work experience not only negatively impacts the future employment prospects of ethnic minorities, it also fails to tap into the deep roster of liberal arts students who, more often than not, have some unique skills and experience which are very applicable to positions within cyber security and technology in general.¹

¹(ISC)² research revealed that the cyber security workforce needs to grow by 62% in order to meet the demands of US businesses today.² Sadly, women hold only 11% of the total number of cyber security jobs, while in the US, only one in seven cyber security roles is filled by a woman.³

---

1. Palmer, Danny. ‘Microsoft Office 365: This targeted phishing campaign uses an odd trick to stay hidden’ ZDNet. 1 Oct 2020. Accessed Jan 2021. www.zdnet.com/article/microsoft-office-365-this-targeted-phishing-campaign-uses-an-odd-trick-to-stay-hidden/.
2. Ranger, Steve. ‘Ransomware is growing: Here are four ways attackers are getting into your systems’. ZDNet. 12 Oct 2020. Accessed Jan 2021. www.zdnet.com/article/ransomware-is-growing-here-are-four-ways-attackers-are-getting-into-your-systems/.
3. Muncaster, Phil. ‘Remote workers could offer Brexit Britain cyber security lifeline’, Infosecurity Magazine, 28 Jan 2021. Accessed Jan 2021. www.infosecurity-magazine.com/news/remote-workers-brexit-britain/.
4. ‘Cyber Security Breaches Survey 2020’, Department for Digital, Culture, Media and Sport, Jun 2020. Accessed Jan 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf.
5. Muncaster, Phil. ‘Remote workers could offer Brexit Britain cyber security lifeline’, Infosecurity Magazine, 28 Jan 2021. Accessed Jan 2021. www.infosecurity-magazine.com/news/remote-workers-brexit-britain/.
6. ‘2020 Cost of an Insider Breach Report’, IBM, Jul 2020. Accessed Jan 2021. www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/.

---

How a humanities background provides real value in cyber security

Trevor Morgan, conforte AG

When you think of the technology industry generally, and in particular the cyber security vertical market, it often conjures up the image of hoodie-wearing software engineers working through the night, making arcane references to code. Or perhaps it’s the frantic sound of typing on keyboards echoing throughout dark smoky rooms illuminated only by pale green light, possibly something reminiscent of The Matrix.