Helping you understand and navigate through the cyber threat landscape

Webinar Writeup Report

TRUST

In this report, we share some of the insights from our latest Cyber Security webinar featuring special guests:

Sam Kennett
Security Expert & Webinar Host
Trust Systems

Leigh Cockell
Guest Security Expert

Glenn Wilkinson
Consulting Hacker

About Trust

Trust is a company that specialises in helping businesses align their goals with innovative technologies. We offer a range of managed and co-managed services and solutions to support small to large enterprises across networking, cloud, digital signage, and cyber security. During our webinar, we collaborated with security experts and an ethical hacker to examine the current trends of cyber threats, assess risks and discuss various approaches to combat cyber threats, these key learnings are summarised in this report.

Cyber Risk, Cyber Reality - “The Fast and the Spurious”

Leigh is a highly experienced information security expert with a wealth of knowledge in IT governance, risk management and control. In a recent segment, Leigh discussed the emerging threat trends in 2023 and beyond, emphasising the importance of understanding risk and adopting a layered approach to cybersecurity threats. He shared tips on identifying and addressing risk, and highlighted the various risk management services available to organisations.

The cyber landscape is constantly evolving, and this evolution is largely in response to changes in how and where we work. In recent years, the pandemic has prompted a shift towards remote working, and hybrid work is now the norm. The next big wave of change is the increase use of Artificial Intelligence (AI) in the workplace. As technology and work practices continue to evolve, this also changes the considerations we need to make when it comes to cyber risk.

We are seeing a rise in complex and frequent cyber attacks. These attacks are becoming more common and are often reported in the media, with significant impacts on reputation, financial losses, and other costs. For example, we have seen attacks on organisations such as the British Library, Leicester Council, Manchester Police, water utility companies, and healthcare providers. Large vendors, such as Microsoft, are also being targeted, as they can provide access to a wider range of sensitive information. These attacks are not limited to large organisations, and we are seeing an increase in the number of smaller companies being compromised. Although these may not make the headlines, they can be catastrophic for small and medium-sized businesses (SMBs) and can even lead to business closures.

The UK's National Cyber Security Centre (NCSC) and the Cyber Security Council oversee cyber attacks in the UK. According to their latest report, there has been an increase in nation-state blocked attacks. These attacks are often carried out by hostile nation-states with a political or financial motivation.

Another trend is the increasing use of AI in cyber attacks. For example, we are seeing an increase in the use of bots and generative AI as part of these attacks.

How is AI changing the landscape?

AI has made it easier for attackers to carry out phishing attacks. With the automation of bot traffic, it has become much simpler to produce phishing emails. This has led to an increase in attacks, with some attackers even claiming to have data on their victims and threatening to report them. As a result, the technical barrier for becoming an attacker has been lowered, making it easier for anyone to carry out such attacks.

What is cyber risk?

Let's talk about the concept of the fast and the spurious. What exactly is a spurious relationship? Well, it's when two events that are not related in any way are connected in some way. Usually, the reason for this connection is an unknown third-party event.

To give you an example, statistics show that cyber attacks happen more frequently on bank holidays. However, it would be a mistake to assume that bank holidays cause cyber attacks, and therefore, ban bank holidays. This is a spurious link, and making such decisions based on a spurious link is not wise.

The truth is that the reason cyber attacks happen more frequently on bank holidays is that people are less able to respond during these times. Therefore, the common element that we should focus on is people's ability to respond, rather than the bank holidays themselves.

Question:

The faster I can respond, the less likely I am to be attacked -

True or False?

Answer: *False!*

How do you protect against an attack?

To improve protection, you should have appropriate defences or remove the targets altogether. What does this mean? It means that when dealing with risks, we should slow down to go faster. We shouldn't make quick, drastic decisions like shutting down the use of the internet as it can have a severe impact on the business. To get it right, you need to work through different scenarios to identify the real gaps and determine what actions should be taken. It's crucial to have representatives from each of your business units at the table, and not just focus on technology alone. You need to understand how the business operates and what risks will affect each part of it.

Have you ever bought a solution and thought it would solve all your security problems?

Many organisations have faced complex situations in cybersecurity. It is a continuous journey and not a one-time solution that can fix everything. When it comes to cybersecurity, it's crucial to align it with the business risks to ensure that the right solutions are implemented to tackle the potential impact. The three elements that are at the core of good security, including cybersecurity, are people, process, and technology.

Why deploy security layers?

"Layering" is an important concept when it comes to security because individual layers can fail. Even though individual protection elements, like firewalls and antiviruses, may prevent opportunistic attacks, they are not foolproof. To illustrate this, let's take the example of a house. A door and a lock may prevent opportunistic attacks by deterring someone from walking in and stealing something. However, a lock is not particularly sophisticated and can be easily overcome by someone determined to get in.

In the same vein, it's important to add additional layers of security to your technology stack, just like you would add an alarm system to your home. An alarm system with cameras and a response team can provide the assurance that you are being monitored and that any breaches will be addressed promptly.

1. We are being attacked
2. We have some way of responding

Cybersecurity involves replacing some physical controls with technology controls, such as monitoring through a platform, network sensors, threat hunting, security operations, and a specialised cyber research team. These measures are necessary because your defences are under constant testing, often without your knowledge. For instance, receiving a phishing email is one way attackers test your defences. However, cyber attacks are more complex than just one email. Hackers can exploit your internet-facing vulnerabilities using automated tools and bots. It's important to ask yourself if you're confident enough that your business is not a viable target for these malicious activities.

Increase in ‘smash and grab’ compromises.

In some cases, groups may not have a sophisticated approach and their goal is to break in as quickly as possible, take as much as they can and then try to extort you. These groups may demand a ransom of $1,000,000, but they have not researched anything about you. They lack sophistication and knowledge, but their actions can cause significant damage.

What can you do?

As a starting point, it's important to ask yourself why you're reviewing your security measures. For many, it's to avoid financial loss. However, there are other factors to consider, such as legal and regulatory requirements that could result in reputational damage. Social responsibility is also a key consideration.

Before you begin assessing your security needs, it's important to identify the most important drivers for your business. Each company is unique and will have different priorities.

If your top priority is to avoid financial loss, you may want to consider obtaining insurance. To qualify for insurance, you'll need to demonstrate that you have the necessary security measures in place. Security frameworks can help to minimise the risk of cyber attacks, especially if you have legal or compliance obligations.

These frameworks provide guidance on best practices and controls for managing and measuring your ability to respond to risk.

According to Gartner, by 2025, 60% of businesses will use cybersecurity as a primary selection criteria when choosing suppliers. This is due to the increasing number of attacks targeting the supply chain. It's becoming increasingly clear that taking cybersecurity seriously is essential in order to be seen as a trustworthy business partner.

Scenarios

Let’s take some real life examples. Here we have broken these down into data locations, where my data is stored. The majority of businesses store data:

- Pieces of the paper in the actual building itself
- More common will be endpoints on the network
- Data centres and the cloud accessing applications

Each of these carry different risks and you need to consider:

Endpoints

- Devices have apps installed, some of might be compromised or not up to date
- Devices can be lost
- Connecting to unsecured networks with people travelling, what ransomware and encryption is in place

Strategies to combat these risks include; cryptic mobile device management, vulnerability management and patching and keeping those machines up-to-date, endpoint detection response or managed detection response to look out for ransomware web content filtering.

Networks carry different types of risk:

- Connectivity loss
- Denial of service attack
- Natural disasters
- External connections into my data centres
- Lateral movement from within
- Exploitation of network vulnerabilities

Strategies to deal with these needs to include backup continuity and disaster recovery to ensure if the worse happens you have some way of recovering.

Cloud has similar, but slightly different risks:

- Risk of people taking over our accounts
- Unauthorised access of data
- Data loss
- People attacking through phishing to try and get a click on the links to give them access
- Insider threats - either intentional or accidental

Strategies to consider are user identity management, MFA, to confirm who it is that's on there, and back up in the cloud. Cloud access controls determine who can get in and in what scenarios.

With all scenarios and risk you need to have plans to address the risk, and you need to test those plans. The test really is to ensure you understand what to do when there is a cyber attack, that your team is ready. This in turn will minimise the damage and financial impact of the attack and provide ways to rapidly recover.

Let's look at an example of the use of endpoint security applying the principles of people, process and technology. For people, we are going to look at SoC and our process instant response on our technology. With the implementation of a SoC service you have cyber security professionals monitoring systems who are trained to recognise tactics, techniques and procedures used by threat actors. When an alert happens they can identify if it's associated with something they recognise. Great, but on their own this is not scalable therefore we have technology that does the same thing in this case, EDR. EDR uses AI that has been trained to look out for tactics, techniques, and procedures that SoC teams know and it builds those alerts into always-on behavioural monitoring. The programme can instantly react and say, ‘hey, it looks like something bad is happening. We need to respond to this’. Then the SoC can give a second opinion. When you combine these it becomes a managed detection response solution.

Combining technology with people drives a instant response process. Understanding what to do when bad things happen and who to get involved will make you more resilient to an attack, at least from an endpoint perspective. Now the challenge is to apply the same principles to other data locations.

Finally, cyber security is a journey, it is a harsh environment. There's no final goal, we need to learn from our experiences. There will be mistakes on the way. You need to adapt and grow, hopefully, this is showing you how you can review the risk in your environment and then start making some of the plans to respond to this.

Hacker Evolution: From Mainframes to Ransomware

About Glenn Wilkinson

When he’s not being a consulting hacker, Glenn Wilkinson is building products to help organisations defend themselves against cyber criminals; a security expert with more than 15 years of experience as an ‘ethical hacker’ Glenn has helped several organisations, from startups to governments and multinational conglomerates address security issues.

What is an ethical hacker?

An ethical hacker is hired to break into an organisation to help them find the weaknesses so they can fix them before the bad guys. Glenn is an ethical hacker. What this means is clients pay for Glenn to break into their systems to find the weaknesses before the real bad guys do and help them patch them and keep their data secure.

In a poll where a large number of executives from small, medium and large organisations were asked ‘What do you think is the biggest risk your organisation?’

Coming in at #3 is cyber risks or cyber incidents. Whilst this covers a broad field it is the only one that is quite specific compared to a pandemic or market developments as these would affect a lot of organisations.

Where it came from and how we got to where we are now gives us some context to what we can do about it.

The history of computer hacking

The history of computer hacking goes all the way back to the 1960s, back when the computer mainframe would occupy an entire floor of a building and were found mainly in universities or very large corporations. At this time computer resources were extremely scarce and if you wanted to run some software or do calculations, you would have to book weeks in advance and the punch a card to gain access. For students is was difficult to access and they soon figured out the most efficient ways to run the software to enable them to get more time on the computers and those elements of the software were called ‘hacks’ and that is where the word hacker comes from.

The term was associated with enthusiastic and skillful computer programmers or users. Between the 60s until the 80s, a lot of development took place, introducing phone systems and bulletin board systems. At this time the perimeter of an organisations network was the perimeter of its physical building. An employee would enter the building, sit down at their desk and turn on their computer, carrying out their work turn it off and go home. The computer stays at the office with the serves in the basement, and the perimeter is well defined. Simple for an IT Manager to turn things off if things are looking odd. Jumping forward to the modern day and that privilege has essentially been blown away. With working from home or anywhere being the norm. This now means an employee needs connectors from home to their corporate network. Now, where is the network boundary? And where is your defence point and what?

Organisations and individuals have shifted their servers from on-premises to the cloud, which essentially means that the cloud is just someone else's computer. However, the question arises, where do the network perimeters lie?

With employees working from home, it is difficult to determine where the network boundary lies and, more importantly, where the defence lies. In addition, servers are no longer located in the basement but are now available through the cloud, which means that the network perimeter is even more difficult to define. Furthermore, the use of devices and smart technology has added a layer of complexity. Smart fridges, washing machines, televisions, fans, and other devices are now commonplace, both at home and in the workplace. A smart coffee machine, for example, needs to be connected to a network to function, and the machine itself might be manufactured in China, with the API connecting it to the network also located in China. As a result, a foreign entity could potentially gain direct access to a corporate network. This is just one example of the challenges involved in defining a network perimeter, identifying network assets, and protecting the network by applying updates and patches.

In Summary the advent of new technologies with added complexity. Hackers are lazy and take the path of least resistance to get to the good stuff. Over the decades hackers have moved from targeting maybe servers and switches and infrastructure in the 90s to, services like web servers and FTP servers, file servers as those get patched and the defenders catch up. Maybe web applications in the early 2000s, WiFi and other network exposure. Hardware or software, and most recently fishing is probably the most method of compromise today, just because it's the easiest and most successful. Hackers would rather send a simple email and you click something and that’s it. - game over.

Story:

There was a person who owned a smart light bulb. They were really proud of it and shared their excitement on Twitter, saying, "Hey, I love my new adapted smart light bulb." Unfortunately, a hacker saw the tweet and knew that the light bulb had some security issues. Using this knowledge, the hacker was able to access the person's laptop through the cloud that controlled the light bulb. Since the light bulb was on the same local area network and WiFi, the hacker was then able to infiltrate the user's company network and gain access to the entire organisation's network. All of this was possible due to a simple, innocent tweet.

This story highlights how technology advancements and connectors have led to increased complexity, making it easier for organisations to fall victim to cyberattacks. In the past, hackers would target the infrastructure of organisations such as servers and switches, but over time, they have shifted their focus to services like web and FTP servers and other exposed network points.

Nowadays, phishing is the most common tactic used by hackers as it is the easiest and most successful way to gain access to sensitive information. Hackers often choose the path of least resistance, opting to exploit vulnerabilities in the system that are not well-protected, rather than trying to penetrate the front door of an organisation's security measures.

The history of ransomware

Ransomware represents a significant risk to SMB's due to its capacity to disrupt operations, incur substantial financial losses, and damage reputations. Ransomware simply explained: imagine someone locks your toy box and says you can't open it unless you give them the candy, you give them the candy, ransom works like that, but for computer files and they want money to unlock it. Ransomware is malicious software that can run on a computer. Normally the Windows computers, when it runs it will gather up all of your files, encrypt them, and present you some kind of message saying ‘Give me some money. In order to get your files back’.

Question:

The first instance of ransomware? Was it five years ago, 10 years ago, 20 years ago, 100 years ago?

Answer:

1989, a malware extortion attack. The user was asked to pay 189 US dollars in order to obtain a repair tool to get their files back. It was a very basic attack distributed by a floppy disc at a conference that encrypted files and present a message. The hacker provided their postal address to send the money in the message, of course this lead the police to them and they were arrested.

Hackers are individuals who are inherently curious, always tinkering and pushing the boundaries of what is considered possible. They are essentially skilled programmers who are passionate about exploring the uncharted territories of technology. From the 1960s until the 1980s, we witnessed a significant boom in technological advancements, and we also saw examples of these new technologies being hacked. For instance, phone systems and bulletin board systems were among the early targets of these curious and resourceful hackers.

Convenience vs Security

Today, individuals and organisations must choose between convenience and security. Businesses must find a balance between convenience and security risks. For instance, imagine a situation where there is no need for passwords - it may seem super convenient, but it is like leaving your office door open. An employee could walk in, sit down and start working without any authorisation. This would create a high-security risk, as anyone could walk in at any time.

What is ransomware?

It is a malicious software that can run on a computer. Normally, when a Windows computer runs it gathers all files, encrypts them, and presents you with a message saying ‘Hey, give me some money and you can have your files back.’

There are two types:

1. Locker ransomware which denies access to the entire system
2. Crypto ransomware which encrypts files

Q&A

Q: Do you see many AI driven cyber attacks?

A: AI itself is a force multiplier. AI isn’t used to carry out the actual attack, but it helps. For example, AI can be used to create really convincing phishing emails. Generative AI is also helping hackers with coding aspects to attacks. Overall AI is lowering the technical barrier to hacking.

Q: Tell me more about BitLocker

A: BitLocker gives you encryption, so that's going to give you some protection in certain scenarios. You know if I lose my machine it's going to delay the likelihood of someone getting the data from there but it's a delay. That's not the ultimate solution. So layer that up.

Q: Experienced their phishing attacks. Advise on how best to treat them? Is there any other blocking domains, numbers, or educating users? What's the best way to deal with those AI phishing attacks?

A: We're in a period of transition right now. Email security companies are at the forefront of this. A lot of them are adapting their protection mechanisms to look out for AI phishing attacks. But what they are having to do is they're having to look at data. So they're actually have to apply AI to the emails coming in, and they're not looking just at the email itself. They're looking at the collection, the whole conversation history. So, is this a normal communication with the recipient you've had? Yes. Is this coming from a normal location and they're using that to build better threat intelligence on things like email security platform. So what you're seeing is the cat and mouse game right? AI has muddied the water. It‘s important to focus on resilience and layering because there's no one final solution. At various points in time one of those things is going to fail for you.

Q: Are hackers reliant on human interaction to access endpoints and servers?

A: Short answer is, no. There are multiple methods, but what a hacker finds effective is to gain access to a system by either tricking or convincing a human to give access. It is what we call social engineering. Hackers like targeting people because sometimes they're a bit easier to manipulate than breaking into a system directly.

Q: Why is it so hard to convince SMBs to invest in cyber protection?

A: This can often be due to SMB's focused on growth, and cyber protection can be seen as a cost. It is reliant on the leaders understanding the real threat that could jeopardised the business, even bring the whole thing down.

Smaller businesses also struggle with having resources. There are so many products and services and tools on the market, it’s hard to know which is the right solution. This issue is exacerbated for SMBs as they potentially don't have a dedicated IT department and security team to figure out what's good and relevant.

Speak to our Team of Experts:

Contact us:

Website

https://www.trustsystems.co.uk/

Email Address

Security@trustsystems.co.uk

TRUST