CYBER-SECURITY

THE SECURYS 20 MINUTE GUIDE

Securys

www.securys.co.uk

bsi ISO/IEC 27001 Information Security Management CERTIFIED

ISO/IEC 27701 Privacy Information Management CERTIFIED

The Securys 20-minute guide to cyber-security

Cyber-breaches make the news every day. The US & UK governments talk about cyber-war as the greatest new threat. The recent rise in international tensions has put data security in the crosshairs.

This guide gives you a high-level overview of the threats you face and the things you can do to protect your organisation.

CONTENTS:

What are the threats?

Viruses and malware

The single most common threat, and one that's been around since the dawn of the computer age, viruses and malware are unwanted programs that use one of dozens of different routes to get onto your computer (or phone, or tablet...). The difference between a virus and piece of malware is only that a virus spreads itself between computers, whereas malware is delivered to your computer from a distribution source of some kind. What matters is not how it spreads, but what it can do once you're infected.

Originally viruses were essentially pranks and their negative effects were a consequence of the resources they used to spread themselves, which would sometimes (and still can) overwhelm the networks they've infected. Then people started adding destructive "payloads" to viruses, still out of no motive other than mischief – it's these payloads that have really evolved over the last couple of decades.

These days the risk isn't usually destruction and the motive is always money. Malware and viruses nowadays usually contain a payload that's designed to install silently on your computer and capture sensitive information – mostly payment card and banking data – and, in some cases, let the criminals take control of your computer. They might do this to try to steal from you directly, but more usually it's so that they can use your resources – your computers and internet connection – to attack others, either by sending out spam or as part of a distributed denial of service attack (see DDoS). When your computer has been compromised in this way, it's known as a bot and is part of a botnet. Infected machines will often "call home" to a server somewhere on the internet to get instructions from the criminals who are controlling the botnet. Occasionally the malware may also use your computer to mine crypto-currency as well, which can not only affect performance but also increase your electricity bill considerably.

Ransomware

This is a special case of the malware/virus threat, and one that has been both prevalent and newsworthy in the last couple of years. The infection mechanism is the same, but the payload differs – instead of destroying your data, or taking control of your computer (although it may do that too), the malware encrypts all of your files, then demands that you pay a ransom in order to get the files back. The ransom is usually payable in an untraceable crypto-currency like Bitcoin. Oddly enough, if you pay the ransom you probably will get a usable decryption key – in other words, you will get your files back – because the criminals know that if they keep up their end of the bargain, people are more likely to pay up.

Viruses and malware can make their way onto your computer in any number of ways. These are some of the most common:

Spam

Unwanted email isn't just an irritant. Often the links in emails connect to websites that will attempt to infect machines; attached files too can contain viruses and malware – and this isn't just limited to program files; nowadays many different kinds of attachment can carry a malicious payload.

Cracked and unofficial apps and games

It's possible to get malware – or unexpected abuse of data – from apps in the official Google and Apple stores, but it's much more likely when "side-loading" from unofficial stores. If you're offered a "free" version of an otherwise paid app, the likelihood is that it will be infected.

Infected media

An easy way to get malware onto a machine is to load it onto a promotional USB stick or DVD. It's surprising how often people will insert media into their computer without having any certainty where it came from or whether it's clean.

Fake websites and compromised real ones

Another key vector is infected websites (so-called "drive-by infections"). Criminals will choose domains that are common typos of real ones, or create very similar-looking sites and manage search results so that they appear at the top of searches. They can also hack real websites and use them to infect visiting devices. It probably won't surprise you to know that porn sites are a common source of infection; in fact this is probably the real main reason that they're usually blocked on corporate networks.

Compromised web ads

Finally there have been a number of examples where malware has been inserted into ads being displayed by legitimate ad distribution networks. These ads then appear on innocent websites and infect anyone to whom the ad is displayed.

What are the threats?

DDoS

One way to attack a company without having to guess passwords or get through firewalls is simply to overwhelm its website, or email server, with internet traffic to the point where it stops working. This is known as a Denial of Service ("DoS") attack. The extra "D" at the front of the DDoS acronym stands for "Distributed": commonly, the required volume of traffic is achieved by using hundreds or thousands of compromised computers – so called "bots" which have been infected with malware – to send or request data at the same time. Having lots of sources makes it much harder to defend against the attack.

Although DDoS attacks are sometimes done just for "fun", they're more often either politically motivated or, once again, performed for money. Not only is it common for popular websites, or companies that are perceived to be reliant on their internet presence, to receive "protection money" demands requiring payment in order to avoid a DDoS, criminals can also rent DDoS services from the cyber-criminal underworld.

Hacking

Although movies and television suggest that hacking is done for amusement by disaffected teenagers living in their parents' basement, the reality is that most unauthorised penetration of company networks is done by organised criminals or nation state intelligence services. The criminals will always have a clear financial motive, whether it's to steal payment card information, obtain money directly by fraudulent transfer or steal information that they can sell on or hold to ransom.

The motives of nation state actors are more varied; their resources mean that a determined attack is relatively difficult to prevent. Far-fetched though it may seem, such attacks are increasingly a part of the threat environment for organisations responsible for critical national infrastructure, for finance and government and, above all, for defence.

Despite its media portrayal, hacking only sometimes involves directly penetrating a network from the outside. Normally one of the other techniques listed above – malware, social engineering, spear-phishing – will be used either to compromise the target organisation or part of its supply chain. Some of the most prominent data breaches of recent years have gained entry via the weakest link in a chain of digitally-connected organisations.

What are the threats?

Phishing and spear-phishing

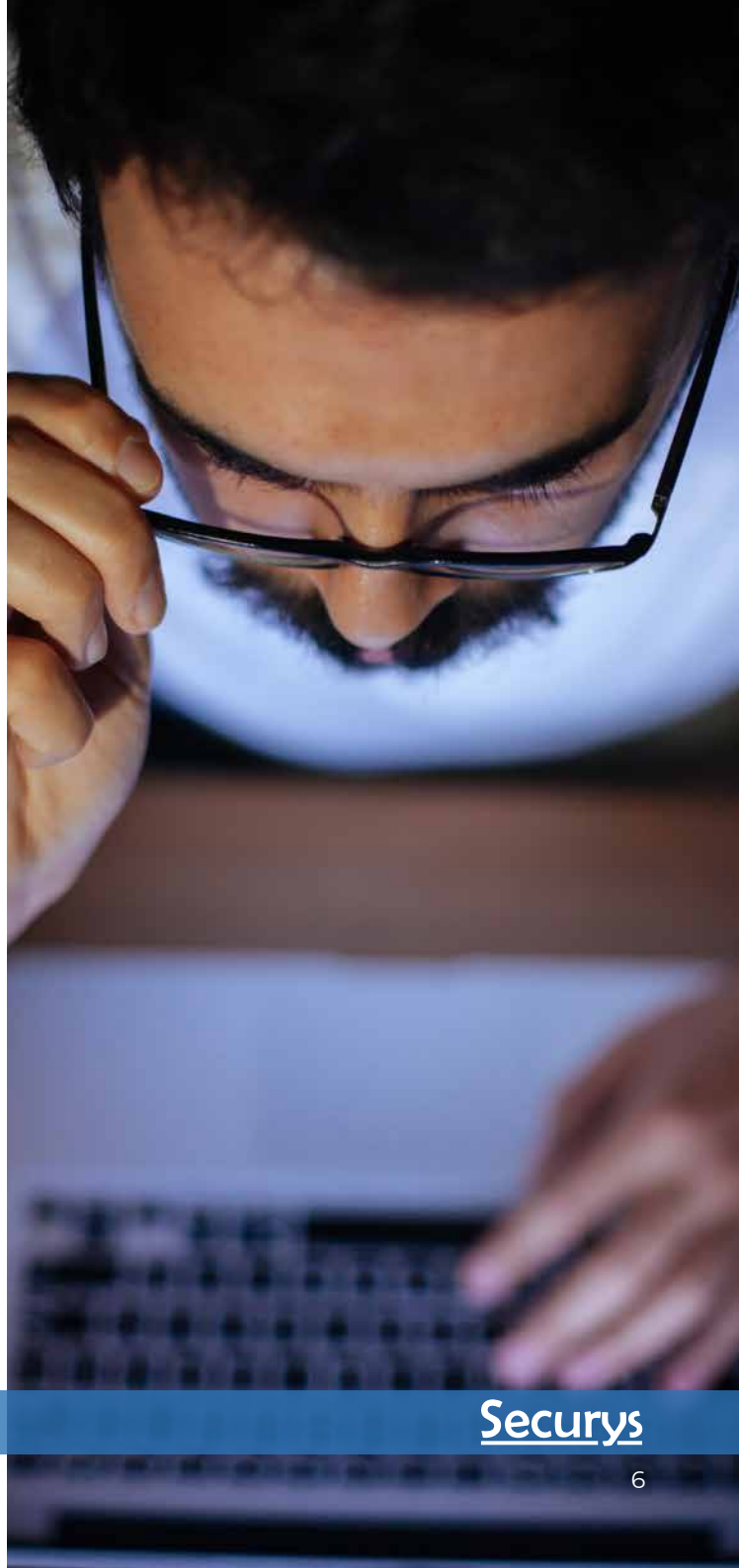
As with most of the risks we now face, this one is all about following the money. What the criminals want is access to your accounts – either directly to your bank accounts or PayPal and the like – or to your social media and other services, where they may find data that lets them steal your identity or helps them hack into your bank or your own computers.

Normally phishing works by sending you a fake email, or sometimes a fake text, purporting to be from a respectable service – your bank, your credit card company, PayPal and other major web services and so on – asking you to go to a website linked in the message. The website will look official, and will ask you for your username and password, and for whatever other sensitive information the criminals think they can get away with. That's the information they later use to compromise your accounts or steal your identity.

Phishing emails are often carefully crafted; they'll use recent events to seem credible, and will try to work on you psychologically to make you act in haste – making it seem like you have a limited time to secure your account, or suggesting that there's a massive unexpected charge to your account, usually timed at the end or beginning of the month so that – if it was real – it might stop your mortgage payment or other regular bills being paid.

Spear-phishing is a more sophisticated version of phishing, usually as part of an attempt to hack into a company network or steal money directly. The criminals will have already obtained some information about you personally, either from social media and sites like LinkedIn, or from a successful phishing attempt. They'll craft something specifically aimed at you – using your name, your position, perhaps the names of colleagues or some update you've recently posted, so that you're less likely to be suspicious and more likely to provide the information they request, or follow their instructions in some other way.

Phishing is also a component of payment fraud – either the email will claim to come from a supplier advising you of new bank details, in order to divert your legitimate payments to the fraudsters' accounts, or it will look as though it's from a senior colleague, instructing the finance department, or a payment clerk, or sometimes their personal PA to make an urgent payment for some apparently credible reason.



What are the threats?

Social engineering

This is like phishing (or spear-phishing) but in person. It can be done by email, but more commonly it's a phone call from someone claiming to be from your bank, or from a recognised company that you may use, or from your organisation's internal IT department. Often it follows a well-publicised hack – not only do the crooks get your basic details from the stolen data, making them sound more credible, but they may represent themselves as working for the company that's been hacked and claim that they're calling to protect you.

Social engineering has become much easier for criminals since the rise of social media. Your public Facebook, Twitter, Instagram and LinkedIn profiles can easily contain more than enough information for a con-man to make a very convincing approach, whether pretending to be a colleague, a friend or a supplier.

This kind of attack can have a number of purposes, but the most common two these days are credential theft – asking for card numbers and PINS – and fake tech support, where the caller suggests that you have a virus on your computer, asks you to give them access to it via a support website and then charges you for completely unnecessary work and software; the software will almost certainly also give them continued control of your computer and let them steal your data and passwords.

Staff negligence and malfeasance

Even though this guide has just listed half-a-dozen different kinds of external threat, the reality is that much of an organisation's risk lies inside its perimeter. The majority of data breaches happen by mistake – human error by your own staff, compounded by weak systems or poor processes. Sometimes the fault lies in ignorance – the more technology proliferates through an organisation, the more opportunities there are to use it incorrectly or unsafely; at other times it's a consequence of acting in haste, and therefore failing to think hard enough about the possible consequences of an action.

Then – however much we'd like to trust all of our co-workers – we have to remember that sometimes people will abuse the privileges they have been given – for monetary gain or out of boredom or in revenge for a perceived slight. Misuse of data and damage to systems perpetrated by staff – especially in the IT department – who've been dismissed or made redundant is a recurrent theme, as is abuse of data by staff with interpersonal grudges or inappropriate romantic interest in co-workers.

What can we do to protect ourselves?

Train your staff

If you do nothing else, you should train your staff in basic security precautions. If you can get them to think twice before opening attachments, following links, providing information to callers – no matter how convincing – and sending money, you will have made significant steps towards protecting yourselves.

Securys offers both on-premises and off-site security awareness training covering the full range of threats and at various levels from basic to expert.

Defend your network and computers

Although training and policy should be your first line of defence, technology also has a role to play. Your investment in defences like firewalls, anti-virus and anti-spam systems and more sophisticated technology like intrusion detection systems and multi-factor authentication should match the risks you face and the value of your data and systems to your organisation.

Securys's CISO-as-a-service offering and our Helpline can give you impartial advice and recommend appropriate technology partners.

Have effective and enforced policies

For training to work you need to give staff clear guidance on what is and is not acceptable, and you should have straightforward, tested procedures in place to cover common security risks. A properly-constructed set of policies not only acts as the basis for your training programme but can also help you comply with regulation like the GDPR and obtain certifications such as ISO27001, CyberEssentials and PCI-DSS.

Of course having policies does nothing unless you enforce them. You should consider establishing an internal audit function or contracting for regular compliance checks.

Securys has a comprehensive policy and procedure library available for licence, and our DPO- and CISO-as-a-service offerings include routine compliance auditing.

Use the cloud – but use it well

Effective use of cloud-based services can be an important part of your strategy. Large cloud providers share the cost of investing in defences amongst all of their customers, enabling you to achieve a level of security you might not be able to afford. Cloud can also simplify your business continuity planning and make it easier for staff to work remotely and flexibly.

Choosing the right cloud and getting the best out of it is not simple. You must manage and monitor your cloud – its ease of access is also a risk if you don't control permissions and users properly – and you need to be sure that your cloud provider is continually updating and improving their security. Even if you have adopted cloud, you still need to train and manage your staff and protect their devices.

Securys can advise you on cloud selection and migration, and our CISO-as-a-service and Helpline offerings can help you stay on top of your day-to-day security monitoring.

What can we do to protect ourselves?

Stay up-to-date

The threat and regulatory environment is constantly changing. If you don't stay up-to-date you risk being caught out by newly emerging vulnerabilities and the latest scams. Whether it's training, software updates, device maintenance or updating policies and procedures, it's a continuous and daily activity.

Securys can help you share the load – our DPO-as-a-service and CISO-as-a-service offerings give you the oversight and advice you need, while our regularly-updated document library helps you stay ahead of regulatory change.

Protect your data

Make sure you have regular backups and that those copies are accurate and accessible. Once you have that sorted, you should look at ranking your data by sensitivity and applying stronger protections where they are needed – including access control and encryption. One of the biggest problems with ransomware is that too many organisations allow everyone to make changes to files, meaning that no matter who gets infected you lose all your data. You're also required by law to have specific protections in place for certain kinds of data – be sure you know what data you have and that you've done what's necessary.

Securys's consultants can map your data and work out how best to protect it. Our DPO-as-a-service can help you make sure it stays safe and is processed in accordance with the law, and our Helpline can answer your questions as they arise.

Manage your supply chain

In many cases it's not your security that's at fault in a breach. Often it will be a supplier – or sometimes a customer – that is first compromised, then the attack spreads to you through that trust relationship. If you have customers or suppliers who have access to your data or network, or whom your staff trust to give instructions, then you need to audit them and assess the risks.

Securys has a comprehensive supply chain audit process, with ready-made security standards and data-sharing agreements as part of our document library. Our CISO-as-a-service and DPO-as-a-service offerings include supply chain auditing and risk assessment.

What if we have a breach?

Planning

However good your security may be, you should assume that you will at some point be breached. Much of what your policies, training and technology will be trying to do is minimise the impact of the breach but once it's happened you won't have time to work out what to do. It's essential that you make a breach response plan, and that you keep it up to date.

Communication

A key part of your breach plan will deal with how you tell stakeholders about the breach. Whom you tell, what you tell them and how will of course in part depend on the nature of the breach, but you need to make sure that you control the narrative and that you comply with your statutory reporting obligations – all breaches should be logged, some will require you to tell the regulator and, in some circumstances, affected data subjects within 72 hours of discovery of the breach. Getting the right message out before any stakeholder finds out about the breach from other sources is critical to minimising the reputational damage that can be the worst part of a breach incident.

Recovery

The other thing you need to do as quickly as possible is return to business-as-usual. The longer the period of disruption or uncertainty following a breach, the greater the impact it will have on your reputation and finances over the long term. Make sure you know whom you'll turn to and what assistance you'll need in different breach scenarios; make sure you have the right contracts in place with appropriate response times, and that you've tested your plan.

Our CISO-as-a-service and DPO-as-a-service offerings include breach management and assistance.

What do the leadership team need to monitor?

Commenting on a data breach at Heathrow Airport Ltd, Steve Eckersley, Director of Investigations at the Information Commissioners Office, said *"Data protection should have been high on Heathrow's agenda. But our investigation found a catalogue of shortcomings in corporate standards, training and vision that indicated otherwise."*

Information security is a board issue. Whilst you'll probably delegate specific actions to managers, the leadership team retains responsibility for the overall management of risk, of policies and of monitoring that controls are effective.

10 of the questions to consider on a regular basis

1. Has the threat landscape changed. If so, how are we responding to that?
2. How is staff awareness of IT security issues and of our policies being maintained?
3. How do we know that staff are complying with IT security and data protection policies?
4. How do we ensure that software is kept up to date, both on user devices and network devices?
5. When were our technical protection measures last reviewed to assure us that they remain appropriate and proportionate to the threat?
6. How do we protect against phishing type attacks?
7. How do we manage our suppliers to ensure that they are not a weak point in our defences?
8. How do we control access to systems and data. How do we monitor this?
9. What new projects are under way and how have we ensured privacy by design?
10. When did we last simulate a security issue response and what did we learn?

How can Securys help?

Securys has a wide range of offerings to help you prevent, mitigate and recover from breaches.

Support available from Securys includes:

- document templates and ready-made policies
- consultancy and implementation
- leadership and staff training
- helpline
- Data-Protection-Officer-as-a-service
- Chief-Information-Security-Officer-as-a-service

Securys

For more information about Securys and our services, please contact us through our website at www.securys.co.uk, or email us on info@securys.co.uk, or call us on 0800 193 8700.