computercentric

Cyber Security White Paper for Customers

Ross Edwards, Computercentric Ltd. Revised 01/09/2019

Computercentric ITS Ltd ▯ 200 Rookery Lane ▯ Aldridge ▯ WALSALL ▯ WS9 8NP
Registered in England and Wales as Company No. 9183046 ▯ VAT No. 201 0595 60

Introduction

We've collated these guidelines and recommendations in order to help our clients avoid becoming the next victim of a hacking or defrauding attempt.

In the last 18 months there has been a major increase in the number of targeting hacking attempts on smaller businesses, our own clients included, with some leading to immediate financial losses and significant disruption to business operations.

Most of these losses could have been avoided if these guidelines had been in place, and carefully followed. We're always cautious about scaremongering, however the reality is that these attacks are now commonplace, and without exaggeration, a daily occurrence for our customers.

It's vital that business owners and managers take steps to minimise the risks to them. We know this is possibly the least exciting document you will read this year, but please persevere, it will be worth it.

We have tried to make this document readable and understandable to an individual with a basic level of technical understanding, so you don't have to be an IT expert to get the gist of what we're saying here. This approach necessitates omitting a decent amount of technical information, so if you find yourself wanting more information or clarification on anything, please talk to a member of our team.

Most Common Attacks

We're using the term "hacking" generally here, however most instances we have witnessed will involve one or more of the following techniques:

- Using email to trick your users into logging in to what they believe to be a legitimate Office 365 website (or other online service), in order to capture their username and password.
- Scouring your user's email history for information that could be used to defraud you or a customer / supplier you have worked with. This usually involves finding a high-value invoice which can be doctored.
- Adding an inbox rule, so that all of your email gets copied to an external email address, so that even if you change your password, the hacker continues to receive copies of your email in order to construct a hacking attempt on you or your customers / suppliers.
- Sending you an email, appearing to come from a known contact, in order to get you to open an attachment, which subsequently and immediately encrypts ALL of your data on your computer and your network. You are then encouraged to pay a fee (typically tens of thousands of pounds,) in order to have your data returned to you.
- Placing phone calls to your accounts department, quoting the names of people such as colleagues, customers or suppliers, in order to appear genuine. These calls might appear to be harmless surveys to determine who your key suppliers are. They can often be followed up by an email or phone call, weeks later, claiming to be from that supplier, and requesting that you amend their bank details for the next payment run, or chasing you for an overdue payment.

This is a far-from-exhaustive list but highlights some of the most common techniques we have witnessed in recent months. It's important to stay vigilant, and to be aware of the latest scams and tricks being used, so that you can protect against them.

The Fix?

Understand that there is no single solution, or piece of software or hardware that you can install to prevent these hacking attempts. It's very much a case of making sure that the minimum level of hardware and software protection is in place.

Whilst there are important technical solutions you should adopt, beyond this, the most important thing you can do, is to educate yourself and your colleagues, and ensure that a set of guidelines appropriate to your risk level is followed.

This is not a pick-and choose list! Where they apply to your business, we recommend you adopt all these guidelines if you have not already done so, in order to minimise your exposure and risk. This list in not in any order by the way. We consider them all important, some more than others, and the order of importance will vary depending on how you do business.

General IT Security Guidelines and Best Practice

1 Get Cyber Liability Insurance

More and more insurance providers are offering this; however, we strongly recommend that you deal with a cyber-liability specialist who can ensure you take the right level of cover for your business.

Speak to us if you need any recommendations on providers of Cyber-liability cover.

Good cyber-liability cover will pay out in various situations, to minimise the financial losses to your business. For example:

- Cover of any losses resulting from extortion or paying a ‘fake’ payee.
- Cover of any losses and direct costs associated with recovering from a data loss or ransomware attack.
- Cover of any losses associated with engaging IT specialists or legal experts, or even marketing advice and reputation management in the event of a data theft.

Please understand, even with cyber-liability cover in place, your insurer will require that you have taken appropriate steps to minimise your exposure. That’s why we encourage you to read, understand and act on these guidelines.

We believe that cyber-liability cover should now be considered ‘normal’, alongside other businesses insurances such as your employers’ liability, public liability and indemnity insurances.

2 Use a Trusted, Commercial Anti-Virus Product

Windows 10 includes a free antivirus product (Windows Defender) however we strongly suggest that this is inadequate for commercial use, as it lacks many of the features that we would consider critical in defending against the types of attacks we are seeing, and none of the management or reporting features that you need.

The bottom line – in business you need to pay for decent, robust commercial-grade anti-virus software. Our recommended product is Sophos, although other options are available. Anti-virus software typically costs only a couple of pounds per month per device and is a ‘no-brainer’ must-have item.

3 Use a Trusted, Commercial Anti-Ransomware Product

Most commercial anti-virus products do not include specific protection against ransomware attacks. This is additional software which looks for the tell-tale signs of a ransomware attack and will greatly reduce the risk of your data becoming stolen and you held to ransom.

Since 2017 our advice to customers has been to deploy a dedicated anti-ransomware product on your network in additional to normal anti-virus cover. The Sophos Intercept-X product is our preferred solutions. We have had no instances of ransomware attacks on clients protected by Intercept-X. Intercept-X is available as an upgrade to the basic Sophos anti-virus product for a small price per device.

4 Ban the Use of Portable Data Devices

With the proliferation of data sharing tools and the general availability of internet access, there is rarely a need to carry sensitive data on a portable USB drive or mobile hard drive.

They are extremely vulnerable to theft and data loss (ask our Government!). We recommend that your internal IT policy forbid their use, unless in exceptional situations.

5 Deploy full-disk Encryption of Laptops and Tablets

Laptops and tablets are theft targets, and usually contain a wealth of sensitive data, or the tools to access the sensitive data. Such devices are now often stolen, not for their resale value, but for the information that is on them. Consider than a laptop in use by a manager or key member of your team might have cost you £1000 to buy, but the data that is on it, or accessible from it, could be worth tens, or even hundreds of thousands of pounds.

With a normal, unencrypted laptop or tablet, the data is easily stolen even if the thief doesn't know your password. However, by deploying "full-disk" encryption, there is no way for a thief to access your data.

Full-disk encryption requires a Windows Professional licence, and whilst it can be manually enabled on individual machines, we recommend it is deployed and managed centrally using the appropriate software for managing device compliance. Such software also offers features like remote wiping of a stolen devices and is available for a small monthly fee per mobile device.

6 Don't be a Data Hoarder

GDPR regulations have encouraged companies to address the risks associated with keeping old documents or old emails, however from experience, we find the majority of clients have identified a legitimate business reason to keep the old data and remain compliant with GDPR rules.

In practice, we would recommend that you put GDPR requirements to one side, and just consider the risks associated with having a large volume of old data on your server or your shared drive, or your eCommerce system. What if this was stolen? What if someone got access to it? What damage could be done with the information you have?

You can greatly reduce the impact of a data theft if you adopt a process for deletion of old emails or documents. Note that you don't necessarily have to delete them, you could just move them to an archive location, access to which is heavily restricted, for example.

If you use Office 365, your provider can set up and roll out policies to automatically delete or archive old emails from users' mailboxes.

There are of course, record-keeping requirements imposed by HMR&C. You must remain compliant with them, but don't share data with people who don't need it.

7 Consider your Physical Security

Most businesses will focus on data stored in their server or in cloud systems, as being a point of risk. However, those piles of documents in archive boxes or filing cabinets are also covered by GDPR and other data protection regulations and are easily overlooked when considering the risks.

It can easily be argued that boxes of data like this are a lot **less** secure than those stored in cloud systems! If you have 'physical data stores', aka filing cabinets, folders or archive boxes, then make sure they are locked away, and appropriate levels of security are in use to safeguard the data they contain.

Physical security also applies to your on-site and off-site computers. Consider the fact that thousands of businesses are now victims of burglary where apparently nothing has been stolen – though in reality the thief was looking for data in order to conduct a future, targeted attack, and was able to get it because you left your PC switched on.

Turn off all computers at night and encourage staff to set their computers to require a password if they are left unattended for more than a few minutes.

Adopt additional physical security where your servers are involved. Like laptops and tablets, forget about the material cost of the servers, this is often negligible in comparison to the value of the data they contain. If your servers contain at-risk or high-value data, they ought to be in a secure room, with restricted access, and covered by a suitable monitored alarm or CCTV system.

8 Consider your Network Access Security

Most businesses will have a 'structured network' of data points throughout the building.

We recommend that these are occasionally audited to make sure there are no 'live' data points in public, or at-risk locations where a malicious user or guest in your business could connect to your network without your permission and attempt to access systems from the inside. If your business is at risk to such attacks, additional safeguards can be put in place to restrict access to the network to known, approved devices.

Also consider your WiFi. If you offer WiFi to staff, visitors or guests, it's vital that the guest WiFi in particular be physically isolated from any sensitive data on your network.

Ensure that any WiFi in use is using the latest security protocols and not older, easily hackable standards such as "WEP". Computercentric or your IT provider can assist with identifying any risks here.

Also consider, (if your WiFi system will support it) time-based access to the WiFi. Many newer WiFi systems will automatically turn themselves on and off at certain times, to reduce the risk of hacking out of hours, by an unwanted visitor sat in a car outside your building.

9 Get in the Habit of Destroying old Data

Like most businesses, you've probably got a pile of old laptops or desktops in the corner of the stock room! Think about what data is on there and how it could be used against you.

Computercentric can destroy old hard drives or other data storage media by shredding them to ADISA / CPNI standards for only £10 per drive. The old-school (free) approach is to drill through old drives to prevent them working, however this does not meet recommended standards for data destruction, and will, more than likely result in some form of injury. I speak from experience.

10 Knowledge is Key

We advise that you conduct regular training with all staff, to help them understand the risks to the business associated with data theft, and to help them recognise when they are being targeted. It is vital that staff be trained how to identify and deal with suspicious emails, letter and phone calls.

Computercentric can offer software which is extremely affordable and allows us to conduct regular reviews of staff to see how likely they are to respond to an email-based "phishing" attack and can subsequently deliver web-based learning to the at-risk members of staff we have identified for you. We can also provide tailored, focussed, client-specific training sessions to staff in small groups, or individuals on a "train-the-trainer" basis. Get in touch to learn more.

Adopt important security policies in your Staff Handbooks or Contracts of Employment, and follow up with regular security updates and training.

Ensure that key members of staff our subscribed to our newsletters or follow us on Twitter and Facebook to ensure that we can alert you to any critical security updates that could be of interest to you. The only way you can stay ahead of hackers is to understand their methods. "Know your enemy" as they say. If you are well-informed about the tricks in use, then you will be in a much better position to spot suspicious activity and deal with it.

11 Protect against Invoice Fraud

The most common financial exploit we have seen involves duping well-meaning, experienced accounts staff into paying a legitimate invoice to the wrong bank account.

Such an attack is usually the culmination of weeks of data gathering or "social engineering" (see #13 below). If you haven't done so already, change your processes to require than any supplier requiring a change of bank details is rigorously verified.

As a minimum, we recommend that requests for change of bank details are verified with a phone call initiated by you, to a known and trusted contact. As an additional measure, consider making a token payment of a £1 to any new bank account that you set up as a payee, and require that a known and trusted contact confirm its receipt before you advance any additional funds to a new payee.

Be aware that fraudsters can appear genuine by sending email from a known email address, or even phoning you from a "spoofed" phone number, so they look like they are calling you from the usual number you're used to seeing!

Train staff to **never** trust an invoice requiring you to change bank details, even if it's from someone they know. Such requests must be validated by other independent means.

Our research suggests that many people believe a "PDF" invoice to be a read-only or tamperproof document, however in reality, it takes only a couple of minutes to doctor a perfectly legitimate supplier invoice to encourage the payer to pay another bank account.

12 Be Careful Who You Talk To

You'd think it would be common sense, but still we find people are easily duped into giving out sensitive data to a phone caller who appears to be genuine. Never, ever do this, and train staff to do the same. Trust no one! Be aware that phone numbers can be spoofed, so a caller can appear to call you from any country, UK region, or even a specific company if they want to.

If you do need to pass sensitive data over any channel of communication, even to known and trusted people, never send the full information over the same channel, on the assumption that it can be intercepted. For example, if you need to email login credentials to a colleague, consider sending the username over email, and the password over an SMS message.

13 Limit the Information you have Publicly Available

We see more and more carefully targeted attempts to steal data which are the result of "social engineering" exploits. This essentially involves a hacker gathering information about your company and its employees from public sources in order to help them appear genuine and trick staff into bypassing usual security processes.

We've witnessed multiple instances of fraudsters calling customers and quoting the informal names of staff, or names of friends, in order to lure staff into giving away sensitive information, or duping staff into making a fraudulent payment after gaining their trust.

It's a sad state of affairs we know, but our advice to clients is now to adopt to a social media policy as part of your employee handbook.

Obvious exceptions would be made in the case of individuals engaged in social media marketing, however as a general rule, we would recommend that you consider:

- Requiring that all employees enforce privacy settings, so that their social media profiles are not visible to non-friends or non-followers.
- Requiring that all employees do not disclose their current employment with your company in their social media profiles. That includes Linked-In!
- Requiring that all employees do not discuss any business-related activity, especially those concerning supplier, customers or colleagues on social media.

14 Adopt a Firewall "Change Management" Process

Regardless of whether you manage your firewall internally, or subcontract it to a provider like Computercentric, we encourage you to adopt a policy for "change management", particularly where firewalls are concerned.

Your firewall is the point at which your IT network connects to the public internet. It's important for your key personnel to understand the risks associated with any firewall tweaks or changes requested by colleagues or third parties such as software suppliers, CCTV companies etc.

You can do this internally, or you can engage your IT provider to do it for you. Computercentric can provide full change-management of firewalls from less than £40 per month, inclusive of regular reviews and security recommendations.

15 Know your Backups

In the case of data theft or ransomware attacks, your only hope for recovery is if your data is properly backed up. We recommend conducting regular checks to ensure that all critical data in included in your backup plan, and that your backup plan is comprehensive enough to meet your needs.

If you engage a provider such as Computercentric to provide backup software, it's vital that you recognise that whilst we will always do our best to advise you, it's your responsibility to make sure that the backup service we're providing to you is effective enough and comprehensive enough to meets your needs.

Like us, most IT providers will conduct a backup assessment to make sure all your important data is backed up, and event conduct regular test restores of your data if you

need it, however please note that we do charge a fee to cover the cost of doing this work, as it's particularly labour intensive.

16 Install your Updates

Microsoft, and providers of nearly all systems will release regular security updates or "patches" for their products. It's vital that these updates be installed, as they resolve any security weaknesses which are identified in their software and reduce the risk of you becoming a victim of hacking.

If you rely on an eCommerce system, there are countless other guidelines which need to be followed, beyond the scope of this document, however the most important one, is to make sure your eCommerce platform of choice is regularly patched and updated in line with the provider's recommendations.

17 Get All Staff Onboard

It's important that staff understand the importance of this stuff! We would recommend that you include a Computer Usage Policy as part of your staff handbook. Whilst such a document is important in conveying the businesses expectations regarding acceptable internet usage and so on, this policy also helps staff to understand the risks they are dealing with, and how best to deal with them.

If you don't have a Computer Usage Policy, we have a template that you can amend and adopt, however we recommend that you speak to a suitably qualified solicitor or HR expert on this.

18 Consider an IT Security Audit

We've provided a lot of information here, which we hope will help you to understand the risks and adopt measures to minimise the risk to your business. However, we recognise that many businesses would rather have someone else do this work for them!

To that end, Computercentric can offer a full security audit of your systems and working practices. To find our more, get in touch.

19 Does it Work?

Note that this guideline only really applies in a limited number of cases, usually where there is a large volume of sensitive data concerned.

It's all very well following this advice, but how do you know if it's working? If you're lucky, then you'll never find yourself falling victim to a cyber attack or scam. However, in some cases, businesses can hold such high-value and sensitive data, that your customers, suppliers or partners who have a stake in your liability, will require some form of testing and auditing to make sure that you know what you are doing!

This usually takes the form of “penetration testing” or “pentesting”. Pentesting processes can be expensive to undertake and coordinate, but not extortionate. They usually involve engaging the services of a so-called “ethical hacker”, i.e. an individual or organisation who possesses the same knowledge and tools as a criminal hacker, but only uses them for good purposes, that being to identify any weaknesses or vulnerabilities in your systems and processes.

If you do find that pentesting is being mandated by a customer or other stakeholder, we can arrange and provide this service for you. As a rule, and for reasons of impartiality, we don’t carry out pentesting work for our own clients in-house, we will bring in a specialised firm to do this for us.

System-Specific Guidelines and Best Practice

The following set of guidelines and recommendations apply particularly to the various business systems in use by your business. We would encourage you to consider each of these systems as individual piles of sensitive data, and make sure you adopt the appropriate level of security, given the sensitivity of the data they contain.

Take some time to think about the different systems you use in your business, we guarantee you will be surprised about how many of these 'data piles' you have got, here is our list to get you thinking:

- Email systems (Exchange or Office 365 probably).
- Accounts software.
- Internal business management / process management software.
- Time / attendance software for clocking-in systems.
- CCTV systems.
- ePOS software for tills.
- eCommerce software that runs your website, or integrates in to it.
- Supplier or customer-provided applications that you are required to use.
- Phone systems and associated software.
- SharePoint, OneDrive, Google Drive, other cloud data stores.
- Internal chat systems (Skype, Teams, Slack etc').
- Note-taking / document sharing applications (Notion, Evernote).
- Web-based project management systems (Asana, Trello etc').

All of these systems should be identified, and we would then ask you to consider the following questions for each of them'

- What data have I got in there that could be used to defraud my business, or a business that I work with?
- How easy is it to get access to these systems?
- Are they as secure as they can be?
- What is my process for ensuring only 'live' users have access?
- Has anyone currently got access to these systems that doesn't really need it?
- Have existing users of these systems got the correct level of permission for what their job role requires?
- Where is the data physically stored?
- Is the data encrypted?
- Is my connection to the system also encrypted?

These questions and your answers to them, will hopefully encourage you to consider any weaknesses in your current setup. For each of the systems you use, we would recommend you undertake the following checks to tighten-up security where each of them is concerned.

1 Enable Multi-Factor Authentication

Especially in the case of highly sensitive data, passwords on their own are no-longer good enough for protecting data.

MFA, sometimes called 2FA for two-factor authentication, is where the system you are logging in to, also requires that you confirm your identify through another independent channel. This often means receiving a text message, or entering a short code sent to you via an authentication app installed on your phone or tablet. This usually only happens the first time you log on to the system on a new device, but on some systems it can be configured to happen every time you access it.

2FA / MFA will **greatly** reduce the likelihood of someone getting access to your data, even if they have got your password. It's a minor inconvenience, but the additional security gained through this process far outweighs the extra headache.

We strongly recommend you enable 2FA / MFA for all services where you have sensitive data. For Office 365, SharePoint and OneDrive, this is easily activated by us at your request, although you may want to consult with employees if you will be requiring them to use a personal mobile phone in order to confirm their identity.

For other systems, check their documentation or contact the provider of the system to find out if 2FA / MFA can be switched on.

2 Enforce Password Security

Make sure that the systems you are using require that your users have suitably complex passwords. We know it can be a pain, and people often choose the most basic level of password complexity for the sake of convenience, however it's too risky. Enforce complex passwords on any systems you use. The headaches associated with having long or complex passwords are easily resolve by #3 below.

3 Use a Password Manager

A password manager is software that allows you to easily start using complex passwords on all the systems you access. It will automatically log you in using your complex password and avoids the need for you to create or remember them. Essentially you remember one master password, which then unlocks all your other passwords.

Take a look at lastpass.com and dashlane.com. These are the most popular platforms and are available from £0 to a couple of pounds per month.

There are of course, risks associated with storing all your passwords in one place. However, the manufacturers of these systems go to great lengths to ensure your passwords are encrypted, to the point where we would suggest that the risks associated with using a convenient password manager, far, far outweigh the risks associated with having weaker passwords that are easier to remember, and easier to crack.

4 Don't have Unnecessary Administrators

Most systems usually have varying permission levels. It's important that users only have the level of permission they need for their job.

In the event of a user's credentials being stolen, the hacker will be limited by the level of permission you have set. If you have lazily granted users higher permissions than they need, then a hacker could easily create a new account for their own nefarious purposes. By the time you have realised a password has been stolen, and then reset it, it's too late as the hacker has now got their own account.

Similarly, if you have identified who needs to have administrator-level access to a system, don't leave this in place all the time. If possible, create a separate administrator-level account for use when it's needed. A hacker is more likely to get hold of the credentials you use every day rather than the ones you use occasionally.

5 Don't have Unnecessary Users

If staff leave, disable their accounts immediately. If it's a system that Computercentric manage for you, e.g. Office 365, inform us immediately when staff leave so that we can do this for you.

Never be tempted to keep former user's accounts open or share their credentials to other staff. Delete the unwanted user accounts and transfer any data that is needed to other current staff.

6 Consider Using IP Location Restrictions

Many web-based systems will offer a feature where you can "lock-down" access by location, so it can only be accessed from your offices or other approved locations. This requires that your location has a static IP address, which most business-grade internet connections will do.

This is an extreme option but is particularly useful where the data is highly sensitive, and there is no need for it to be accessed from various locations.

Please note that this is not normally done with Office 365 as it greatly reduces the usefulness of your email system for remote workers, that said, it can now be added, albeit at extra cost if your business model would support this way of working, if for example your staff generally operate from a small number of locations and don't need to access email or documents off site.