Coretek GROUP

Whitepaper

Security Series.

The 7 Biggest IT Risks to Finance Companies (and how to prevent them)

Address

Coretek Group
Unit 7 Gardeners Business Park
Plaitford
SO51 6EJ

Phone

Phone: 0800 304 7444

Online

Email: support@coretek.co.uk
Website: www.coretek.co.uk

Table of Contents
Whitepaper

Overview
Introducing the 7 Risks

IT security is vital for any organisation, as businesses increasingly rely on technology to do their jobs. A recent survey* showed that in just one year, 46% of UK businesses fell victim to cyber crime, so it is vital to have suitable security in place.

For finance companies, the stakes are even higher due to the valuable and sensitive nature of their data and all the legislations they need to comply with. The financial industry is also among the most targeted by cyber criminals.

We have put together this whitepaper to help businesses in the finance industry quickly spot the biggest IT security risks and how to prevent them.

01. Risk One
Phishing & Whaling Attacks

01

What's the risk?

Phishing is a set of tactics hackers use to encourage targets to unwittingly download malware or divulge passwords or financial information.

Tactics include phoney emails that request personal data and fake websites that resemble official portals your staff frequently use to steal login information. Cybercriminals have become more advanced and can now “spoof” email addresses. This means that even if you check the sender's email address, sometimes it can appear to be from the correct person.

Whaling is similar to phishing but the cyber criminal will impersonate a senior member of staff, often to try and extort large sums of money by deception.
Members of your finance department and senior executives should be particularly vigilant to this kind of attack.

How can I prevent it?

The first step to counter this is education. Make sure all staff are made aware of spoofing and phishing with regular training. Make sure you have internal processes that put additional checks in place. For instance, if anyone is asked to make a payment via email, ensure this is always verbally confirmed by the finance director before actioning the payment.

Having decent email filtering in place will prevent most spoofed emails from reaching your inbox but it is still important staff are aware of the risks.

Finally, don’t forget to put in measures to prevent unauthorised access from within your organization. Make sure adequate permissions are in place to stop users from accessing files, folders and information they shouldn’t.

02. Risk Two

Viruses, Malware & Ransomware

02

What's the risk?

Malware is a catch-all term for malicious software that hackers use to wreak various forms of havoc.

That may include monitoring keystrokes to steal passwords, infiltrating secure databases, and even taking control of your IT infrastructure. Ransomware is a type of malware that hackers use to block access to your private data.

Hackers often demand a ransom payment from organisations to restore your seized data. A very well known example would be the Wannacry virus that caused vast disruption to various businesses and public services in 2017.

How can I prevent it?

The first step is to ensure that you have business-grade anti-virus protection and this is kept up to date. At Coretek, we have carried out an in-depth analysis of all the AV providers and found Webroot to be the best mix of price, protection and performance.

Keep all your software up to date including your operating system, to ensure that the latest security patches have been applied. Your IT department can centrally deploy updates to all machines using tools like WSUS and PDQ.

Educate your staff about the possible causes of malware such as the dangers of clicking on suspicious email links, downloading software applications without IT approval and checking websites are legitimate and SSL protected.

Additional tools such as AppLocker can block users from installing unauthorized software and your company firewall can block access to malicious websites or categories.

03. Risk Three
Weak Passwords

03

What's the risk?

Strong security begins with strong user accounts. If your users have weak, insecure passwords that can be easily guessed or cracked then you will be leaving your business wide open to external attacks. This applies to your internal network and any external, cloud-based systems or websites.

Hackers use automated tools to 'guess' usernames and passwords to gain access to accounts.

Bots are typically able to try thousands of passwords in seconds, and once they've entered a successful combination, give hackers complete access to the user account. This shows to vital it is to make sure all user accounts are secure.

How can I prevent it?

By enforcing a password policy, you can set a minimum set of password requirements. This would include having

a complex password with at least 3 different characters (upper, lower, number, symbol), a minimum length of 8 characters, is changed after a certain number of days and is locked after a set number of failed attempts.

Using the same password for multiple accounts should be avoided and where possible, secure password databases can be used to store passwords in an encrypted form. There are several options available including KeePass, Lastpass and Roboform.

Where possible, enable Multi Factor Authentication, which requests an additional form of authentication, such as a code generated from a secure key or mobile phone app.

04. Risk Four
Email Based Attacks

04

What's the risk?

Email accounts are among the most important areas to keep secure.

Email is one of the most common mediums used by hackers for identity theft or spreading viruses, as well as the phishing and whaling attacks discussed in risk 1.

So, be vigilant and follow the steps below.

How can I prevent it?

A comprehensive email filtering solution will protect against spoofed emails, email-borne viruses and malware.

As well as protection against viruses and malware, email filtering keeps spam in check, helping staff be more productive.

There are several options available.

We offer email filtering as part of our SecureSuite Email package, which is built on technology from the industry-leading Barracuda Networks.

Multi Factor Authentication is a great option to provide an additional level of security to your user's email accounts.

Consider investing in a good email archiving solution for situations where email is lost or accidentally deleted. We include email archiving in our SecureSuite Email package.

Finally, as with all of the other risks, training is vital to make sure staff are aware of the dangers and to help advise staff on how to spot the signs of a malicious or untrustworthy email.

"

The security stakes are even higher with finance companies due to the valuable and sensitive nature of their data and all the legislations they need to comply with. The financial industry is also among the most targeted by cyber criminals.

05. Risk Five
Mobile Devices

05

What's the risk?

People are more mobile than ever and remote working has vastly increased over the past few years. As your staff may not always be working in the office, it is important to consider how their mobile devices, such as laptops, tablets and mobiles are protected.

These may not be covered under your network security and are a higher risk of loss or theft.

It is important to stop your sensitive data from falling into the wrong hands by securing these devices.

How can I prevent it?

Mobile company devices should be monitored and managed, just like any other device.

An MDM (Mobile Device Management) system can enforce a baseline level of security, keep devices up to date and track and remotely wipe devices if they are lost or stolen.

Devices need to be protected by a strong password (see Risk 3) and have the latest updates installed.

In addition, hard drives should be encrypted to stop unauthorized access to the data contained on them.

Encryption can be enabled on all Windows 10 machines and there are options for Mac OS and mobile devices, including iOS and Android.

Staff who are assigned a mobile device should be asked to sign an acceptable use policy, that will ensure they use the device with care, for work purposes only and do not install unauthorised software.

05. Risk Six

External Attacks to Your Network

06

What's the risk?

Just like you protect your computers with anti-virus software, it is important to protect your entire network as well. It is even more important.

External attacks such as DDoS attacks can target your critical infrastructure, aiming to take your IT systems, network, or website offline for an extended period.

Hackers often use the combined processing power of multiple malware infected computers to bring down major IT systems, disrupt mission critical operations or get access to vital company data.

How can I prevent it?

Once you have a good level of protection for your devices as covered under the previous 5 risks, you need to extend this to your infrastructure including network devices and servers.
Your servers should meet a minimum level of security, including having a supported and up to date operating system. We also configure many security settings to further improve server security including limiting services on key servers (Domain Controllers) and disabling default administrator accounts.

Even for smaller organizations, it is important to protect your network from external attacks with a business-grade firewall that offers several features such as advanced threat identification, assessment, and filtering tools to monitor for potential attacks.

The price of firewalls range from a few hundred pounds to hundreds of thousands, depending on the amount of traffic it needs to handle. Coretek recommends SonicWALL as they are a recognised leader in security.
Finally, for extra peace of mind, we recommend carrying out regular penetration (PEN) tests, where an external company will test your level of security for you.

07. Risk Seven
Physical & Building Security

07

What's the risk?

Our final risk is the one often forgotten, but poor physical security is just as big a risk as those mentioned above.

Without putting adequate physical security in place, you are putting your IT system at risk from both internal staff (whether this is malicious or accidental) and external parties trying to gain access to your premises.

How can I prevent it?

Access to key IT infrastructure devices such as servers, firewalls, switches and storage devices should be restricted to only senior members of your IT team with designated access.

Access should be physically prevented by using locked rooms and/or cabinets with keys or keycodes.

Access control is an excellent option for protecting your location and monitoring access in and out of your building, whether this is a code, a keyfob or a fingerprint scanner.

In addition, your site should be well covered both internally and externally by a CCTV system. This acts as both a deterrent and way to monitor or prove activity after the fact.

It may also be suitable to employ security personnel or agnecy to monitor your premises, as well as having an alarm system.

By putting in suitable security measures, you will greatly reducde the risk of your buildings being targeted.

Summary

It's time to improve your IT security

Checking the 7 risks above and putting the recommendations in this guide into action should vastly improve the IT security of any finance business.

If you have any questions about how to implement any of the advice given in the guide, do not hesitate to contact Coretek:

Call: 0800 304 7444
Email: enquiries@coretek.co.uk

How good is your IT security?

We have put together a free scorecard that checks all key areas of your IT security. In under 5 minutes, you will get your personalised report which provides a score in each area and exactly what you need to do next to improve.

Our scorecard includes the following:

- Answer 20 questions and get your scorecard
- Free of charge – no strings attached
- Scorecard takes less than 5 minutes
- Benchmark your business in all key areas of IT security
- Tailored report with specific actions to improve your score

How does your business score? Take the scorecard now and find out.

* Survey from the following source: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020#chapter-2-profiling-uk-businesses-and-charities

Coretek GROUP

The core of your business IT.
Coretek Group

Whitepaper
www.coretek.co.uk