THE BUNKER

Part of the CYBERFORT group

ARE YOU THE WEAKEST LINK?

HOW SENIOR EXECUTIVES CAN AVOID BREAKING THE CYBERSECURITY CHAIN

THEBUNKER.NET

INTRODUCTION

As a senior executive your level of responsibility and privileged access to valuable company information make you a prime target for hackers, phishing scams and fraud. This means you may unknowingly be the weakest link in your organisation's cybersecurity chain, especially if you have, or are in the process of, migrating all or part of your IT infrastructure into the cloud. Professional cybercriminals are extremely resourceful and there are many ways they can access to your personal data and compromise any associated accounts. Once this happens there could be serious consequences for yourself and the organisation you represent.

Fortunately, having a solid understanding of digital security best practice, ensuring all staff are regularly provided with up-to-date training programmes and choosing the right stack of digital systems and services, will ensure you are fully-equipped to defend against any potential threat, targeted attack or data breach. Adhering to these simple rules on a daily basis will also result in numerous long-term business benefits, encouraging growth and a long-term reduction in operational costs.

SUMMARY

UNDERSTAND
the threat
landscape

CHALLENGE
your ideas of the
risks you pose

TAKE ACTION
to ensure no
weak link

SECURE
your cloud
solution

UNDERSTAND

UNDERSTANDING THE THREAT LANDSCAPE

Rapidly accelerating technological advancements in the form of powerful mobile devices, Artificial Intelligence (AI), the Internet of Things (IoT) and cloud architecture are enabling enterprises of all sizes to become highly efficient by facilitating communication and collaboration not possible ten years ago. This hyperconverged digital ecosystem (commonly referred to as industry 4.0) can be a blessing or a curse to anyone taking advantage of the many systems, applications and services readily available, however, the combination of legacy systems, cloud services and the proliferation of mobile devices is creating complexities and new entry points that can be exploited by cybercriminals. Left unchecked, this could have serious consequences for any commercial enterprise.

> **"REPLACE THE WORD 'CLOUD' WITH 'SOMEONE ELSE'S COMPUTER', AND THIS WILL GIVE YOU A BETTER UNDERSTANDING OF WHERE YOUR DATA IS STORED"**

Cybercrime is on the rise, with big data and cloud adoption creating new opportunities for adaptable hackers who can operate from anywhere with a standard internet connection. Over the last two years, the Information Commissioners Office (ICO) has received a 75% increase in reports of UK data breaches, according to research by risk solutions provider Kroll, while supermarket retailer Morrisons is currently facing a muti-million pound compensation claim after losing its appeal over the 2014 breach of payroll data. Many organisations perceive the cloud to be a 'silver bullet' that removes the complications of running IT systems, but Simon Fletcher, Managing Director of Arcturus, rejects this misconception and explains what it actually is: *"We have a saying in our industry: replace the word 'cloud' with 'someone else's computer', and this will give you a better understanding of where your data is stored."*

With damage relating to cybercrime projected to hit $6 trillion annually by 2021, according to Cybersecurity Ventures, and Juniper Research calculating the total cost of data breaches expected to reach $2.1 trillion by 2019, now is the best time to assess the digital behaviour of all staff and reinforce the organisation's cybersecurity chain.

THE TOP FIVE MISTAKES OF SENIOR EXECUTIVES

1. NOT REALISING THEY ARE A PRIME TARGET FOR CYBERCRIMINALS
2. VIEWING CYBERSECURITY AS THE RESPONSIBILITY OF THE IT DEPARTMENT
3. BELIEVING SECURITY THREATS ARE EXTERNAL AND NOT INTERNAL OR ACCIDENTAL
4. THINKING A CLOUD PROVIDER IS RESPONSIBLE FOR BACKUP AND SECURITY OF ALL INFORMATION
5. FAILING TO USE CLOUD HOSTED EMAIL SECURELY

CHALLENGE

MISTAKE #1 NOT REALISING THEY ARE A PRIME TARGET FOR CYBER CRIMINALS

Senior executives and board members are prime targets for hackers, despite many believing themselves to be immune to any potential cyberattack due to their elevated position. Ironically, this seniority and access to sensitive information makes them an ideal victim, with their personal accounts being extremely valuable assets to exploit.

> **"SENIORITY AND ACCESS TO SENSITIVE INFORMATION MAKES [A SENIOR EXECUTIVE] AN IDEAL VICTIM, WITH THEIR PERSONAL ACCOUNTS BEING EXTREMELY VALUABLE ASSETS TO EXPLOIT."**

The open availability of company data on the internet enables cybercriminals to deploy a variety of creative and sophisticated methods to infiltrate a corporate network. Professional hackers and adversaries will usually do a thorough investigation into a senior executive or board level director, including full analysis which could entail in-depth monitoring of the company website and associated social media accounts (including employees and their extended networks) Professional hackers and adversaries will. usually do a thorough investigation into a senior executive or board level director, including full analysis which could entail in-depth monitoring of the company website and associated social media accounts (including employees and their extended networks).This allows them to gather data that can be used to decipher passwords or design highly convincing spearphishing emails. In 2017, spear phishing emails were the most widely used form of attack, deployed by 71 percent of cybercriminals, as evidenced in Symantec's Internet Security Threat Report. These messages usually appear to be from close friends, family members, co-workers or clients and may include specific requests to send sensitive data or contain malicious links that could install a worm, trojan, or malware onto the hosts PC.

CHALLENGE

MISTAKE #2 VIEWING CYBERSECURITY AS THE RESPONSIBILITY OF THE IT DEPARTMENT

Senior executives and board-level directors generally consider digital security to be outside their remit, despite organisations embarking on cloud migration and cost-reduction initiatives. These processes are reducing reliance on in-house IT teams and on-premises legacy equipment by transferring digital infrastructure to a Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) model. This includes data storage, email and popular workplace collaboration tools, with many now opting for a publicly available cloud solution that hosts their suite of customer experience products and services. Shadow IT is also a factor with many staff procuring their own apps, taking data outside of the company firewall and away from the control of the IT department.

Unfortunately, with the hyperconvergence of big data if one account is compromised, a hacker could theoretically gain access to all connected data, systems and applications and potentially infiltrate their customers' devices and networks. This means that IT security has now become the remit of all individuals, especially those in the highest positions of each department and senior executives need to take ownership for IT security best practice in their day-to-day behaviour. Once this has been communicated across the board, it can be promoted as part of a standardised corporate security policy.

> **"IT SECURITY HAS NOW BECOME THE REMIT OF ALL INDIVIDUALS, ESPECIALLY THOSE IN THE HIGHEST POSITIONS OF EACH DEPARTMENT "**

CHALLENGE

MISTAKE #3 BELIEVING SECURITY THREATS ARE EXTERNAL AND NOT INTERNAL OR ACCIDENTAL

It is easy to think of a cybercriminal operating from a dusty basement in a foreign country, but the truth is a lot closer to home. According to risk solutions provider Kroll, 88% of data breaches in the UK are the result of human error, with only 12% coming from malicious attacks. Worryingly, within the health sector, 58% of healthcare system attacks involve inside actors, as revealed in Verizon's 2018 Protected Health Information Data Breach Report.

> **"60% OF DATA BREACHES WERE CAUSED BY MEMBERS OF STAFF EITHER ACCIDENTALLY EXPOSING INFORMATION OR ACTING WITH MALICIOUS INTENT AGAINST THEIR ORGANISATION"**

There are two types of internal threat: the 'insider' and 'third party'. An 'insider' is an individual who is actively employed by the organisation, while 'third party' could be an external vendor or supplier who has been granted access to the digital infrastructure of a business. It is possible they may be unaware they have been targeted, or they could be actively working to undermine the company's security. This could be a disgruntled employee or a corporate espionage agent for hire trying to access sensitive data for personal financial gain. There is also the issue of staff losing mobile devices, USB sticks and external hard drives or someone plugging in a rogue storage device containing malware that could infect an entire network.

IBM's X-Force® report found that 60% of data breaches were caused by members of staff either accidentally exposing information or acting with malicious intent against their organisation. Depending on their seniority, this could provide access to all internal databases and connected applications and the systems would not be configured to defend against this type of breach. The fact that a cyberattack is more likely to originate from within an organisation should prompt senior executives and their staff to think about how they are engaging with colleagues and partners and if there are systems in place to monitor who is accessing the network.

MISTAKE #4 THINKING A CLOUD PROVIDER IS RESPONSIBLE FOR BACKUP AND SECURITY OF ALL INFORMATION AND CONNECTED DEVICES

Popular cloud providers including Amazon and Microsoft are helping companies to streamline their operations and reduce capital expenditure, but the nature of public and hybrid cloud environments in which vast amounts of data resides outside the protection of internal systems makes it a perfect entry point for cyber criminals to exploit. When properly configured, the cloud offers a highly secure and cost effective platform to defend against most threats and malicious attacks. It would be expensive and time consuming to replicate this level of agility on-premises, especially for SMEs, but a lack of clarity around who is responsible for protecting and backing up these newly defined network perimeters combined with confusion over company wide security controls are inadvertently creating new vulnerabilities.

> "WHEN A COMPANY USES ANY TYPE OF COMMERCIAL OR EXTERNALLY HOSTED CLOUD SERVICE... IT OPENS THAT DATA TO A WIDER COMMUNITY"

Despite many companies opting for SaaS, gradually reducing their on premise hardware and reliance on internal IT teams, many still consider it being managed on-site, creating a false sense of security.

There is a lot of misunderstanding about migrating to the cloud, including the effect on company-wide security procedures, the provider's data retention and backup policies and how this impacts business continuity plans. Unless stated, cloud providers do not guarantee complete system security or data backup procedures as standard and there should be a full understanding of the SLA.

The cloud is in the public domain. When a company uses any type of commercial or externally hosted cloud service (including any Microsoft Office 365 application) it opens that data to a wider community, extending the infrastructure of systems and connected devices outside the physical confines of the business. It also externalises the responsibility of IT administration from a single in-house department to a managed services provider (MSP) or cloud vendor, meaning appropriate security and privacy controls will not be established unless configured. Additionally, it is important to understand that Microsoft's cloud services do not automatically backup files, folders or documents and therefore it is the responsibility of the end-user.

CHALLENGE

MISTAKE #5 FAILING TO USE CLOUD HOSTED EMAIL SECURELY

One of the biggest areas of vulnerability for any company is email, with most employees' mailboxes now hosted, stored and managed in a public cloud environment. This open access availability can be exploited by hackers and according to Verizon's 2018 Data Breach Investigations Report, 92.4% of malware is delivered via email, as a business mailbox is a repository of highly valuable information pertaining to the company, colleagues, partners and customers. Yet many senior executives may not realise that their email behaviour could be exposing the entire organisation to a variety of external or internal threats. Common mistakes include sending and receiving Personally Identifiable Information (PII) via email (including names, addresses and bank details) and using the same password for email, cloud services, PC login and VPN access

> **"AN UNSECURE [EMAIL] ACCOUNT COULD BE THE ACHILLES HEEL OF A BUSINESS"**

Email is the most commonly used cloud communication platform and it is highly likely that an unsecure account could be the Achilles heel of a business. The Cisco Cybersecurity Report 2018 found the most common types of malicious files are in Microsoft Office formats, including Word, PowerPoint and Excel. With cloud services now in a publicly shared ecosystem (Office, OneDrive, SharePoint) and secured by a single password, a hacker can access to all connected data, documents and devices and theoretically take control of the entire network. This could lead to any type of ransomware and Distributed Denial of Service (DDoS) attack that could damage an organisation's entire infrastructure and will cost a considerable amount of time, money and resources to resolve, probably resulting in long-lasting reputational damage.

SO THAT IS THE BAD NEWS... BUT FEAR NOT, THERE IS GOOD NEWS!

GET YOUR OWN HOUSE IN ORDER AND LEAD BY EXAMPLE

A STRONG, 'SECURITY-FIRST' CULTURE MUST START AT THE TOP. SENIOR EXECUTIVES PROMOTING A PROACTIVE APPROACH TO CYBERSECURITY ACROSS THE ENTIRE WORKFORCE IS THE BEST WAY OF PREVENTING A DATA BREACH, MALICIOUS ATTACK OR UNAUTHORISED ACCESS (EITHER INTERNAL OR EXTERNAL). EACH EMPLOYEE, FROM THE OFFICE JUNIOR TO THE CEO, HAS A VITAL ROLE TO PLAY, AND FOLLOWING THESE STEPS COULD PREVENT SOMEONE FROM UNINTENTIONALLY BECOMING THE WEAKEST LINK IN THE SECURITY CHAIN.

THERE ARE SIX SECURITY AREAS SENIOR EXECUTIVES MUST PRIORITISE TO ENSURE RESILIENCE ACROSS THEIR ORGANISATION.

ACTION

1. SECURITY IS A BOARD LEVEL ISSUE WITH SENIOR EXECUTIVES DRIVING AWARENESS

In the past, senior executives relied on their IT department to oversee digital security, but with cloud becoming standard, leadership need to set an example by adhering to a strict set of guidelines and prioritising a security first mentality across the entire organisation.

After recognising senior management are a primary target for resourceful cyber criminals and therefore equally responsible for maintaining security, a clear set of rules and guidelines should to be agreed on and implemented with the focus on data minimisation, password best practice and GDPR compliance. This should be devised in coordination with security experts, IT professionals and digital consultants to ascertain the exact level of protection required and will support a preventative strategy that reduces the probability of a careless employee leaking data through poor housekeeping, weak passwords or a compromised device.

2. UPDATING IT SECURITY CONTROLS IN-LINE WITH CLOUD MIGRATION AND NETWORK EXPANSION

Security must keep pace with cloud adoption. When a company embarks on a cloud migration, all senior executives need to ensure they have a thorough understanding of the SLA, revising existing security protocols in line with this to include polices on security, data retention and backup. The provider's security guidelines need to be clearly defined, with all associated profiles, settings and access privileges properly understood and configured. A cloud provider specialising in data protection and backup is beneficial for companies that lack the resources to manage security and should include full stack shielding and backup across all associated applications, devices and Application Programming Interfaces (APIs). Selecting the most suitable provider and understanding their unique position is the most effective way of combating any potential threats looming on the horizon. However, a suitable firewall and anti-virus solution will still need to be managed on-site and installed on all connected devices, with whitelisting and device privilege controls to safeguard all data in-transit. A holistic and cohesive company-wide security framework that clearly defines who is responsible for managing the security settings of both cloud services and the on-premise infrastructure will alleviate confusion and reduce the likelihood of the system being compromised.

3. ARRANGE FUTURE PROOFED SECURITY TRAINING PROGRAMMES TO UPSKILL ALL EMPLOYEES

System security is not a single task that can be completed and forgotten about, but an ongoing process that requires policies and training programmes to be regularly updated. This requires close collaboration between senior executives especially CIOs and CSOs working alongside internal or external IT teams. According to Cisco's Cybersecurity Report 2018, '*User training, accountability, and the application of email security technologies, remain crucial strategies for combatting these threats.*'

With cloud and email being the most common threat vector for cybercriminals to exploit, it is vital that all staff are given training that will ensure a security first mentality. Educating employees with a solid understanding of the current threat landscape and explaining how hackers operate will ensure best practice procedures are upheld. This includes making sure that staff always use a variety of high strength passwords and that two-factor authentication checks are in place when dealing with sensitive information. It should also be acknowledged that individuals who have left the organisation may still have network access and therefore clear employee exit procedures and checks need to be in place.

4. ENSURE DATA MINIMISATION AND SEGMENTATION ACROSS THE ORGANISATION

The new GDPR directive has brought data regulations and compliance into the spotlight with its emphasis on best practice and data minimisation. Being aware of the legal requirements is a good start to thinking about how to acquire, store and share sensitive information pertaining to staff, partners, or customers. There should be an understanding of the cloud provider's policy on this issue and everyone must ensure that PII or financial transaction data is never sent, received or saved via email or attached in spreadsheets, as this is a common entry point for hackers to exploit. One solution is to centralise all sensitive data into a file storage platform secured by a strong password and either two-factor or biometric authentication.

As flexible working becomes widespread, it is common for staff using personal devices to remotely connect from any location. Although this can greatly improve operational agility, it creates a new set of risks, with wireless routers, local networks and unsecure devices being a weak link in the security chain and providing easy entry-points for opportunistic cybercriminals. Instead of prohibiting the use of mobile devices and remote working, simply implementing sufficient end-to-end security controls, network separation and Mobile Device Management (MDM) software will prevent individuals being compromised through their personal hardware or home networks.

5. RUN PENETRATION TESTING AND RED TEAMING TO IDENTIFY WEAK POINTS

'White hat' hackers, 'penetration testing' teams and 'red teaming' are some of the ways an organisation can get an overview of their digital infrastructure with detailed insights into any potential vulnerabilities. Penetration testing is the most effective method for identifying areas of weakened network security, vulnerable entry points or individuals with poor security habits. This usually entails hiring a cybersecurity expert to focus on a particular area of the business such as a specific application, system, location or department. It is highly advisable to run 'pen tests' in the first instance to provide a consolidated list of weaknesses and attack vectors observed during the assessment.

Once completed, companies could consider a Red Team to gauge resilience against a broad scope of attacks. Red Teaming services deploy an experienced group of ethical hackers to emulate what a cybercriminal would do, including using surveillance, social engineering, phishing and network wide analysis to test a company's digital defences. Hiring external teams of security professionals to run regular tests on all applications and associated devices will ensure any vulnerabilities are quickly identified and remedial action can be taken immediately.

> **"AN EXPERIENCED GROUP OF ETHICAL HACKERS [CAN] EMULATE WHAT A CYBER CRIMINAL WOULD DO, INCLUDING USING SURVEILLANCE, SOCIAL ENGINEERING, PHISHING AND NETWORK WIDE ANALYSIS TO TEST A COMPANY'S DIGITAL DEFENCES. "**

EVERY BUSINESS SHOULD HAVE ITS HEAD IN THE CLOUDS

SECURE

IMAGINE TRYING TO DEFEND A CASTLE WITHOUT KNOWING THE WEAK POINTS IN THE DEFENSIVE WALL, WHICH DIRECTION THE ENEMY MAY COME FROM OR WHAT WEAPONS THEY INTEND TO USE.

Surprisingly, this is the position most companies are in when trying to protect themselves against potential cyber-attacks but reviewing corporate security policies, with a focus on people, premises, processes, systems and suppliers will provide valuable insights into which areas to improve.

In addition to championing a 'security first' culture and ensuring staff are using email responsibly, choosing the right cloud, data centre or colocation provider is one of the most important decisions a business will make in the coming years. The wide variety of vendors and services available can be confusing but consulting trusted IT professionals and selecting a company that prioritises security and backup will strengthen protection levels against any potential cyberattack or data breach and ensure data remains secure. When selecting a cloud provider, ensure that they offer:

- A fully managed, ultra-secure IaaS service, including 24/7 data inspection, threat protection and network monitoring
- Secure hardware facilities with an uninterrupted power supply for constant connectivity of mission critical systems and zero down-time.
- Industry accreditations, strict compliance with revised standards and frameworks designed to uphold GDPR regulation and PCI DSS audits.
- An on-site dedicated technical support team of industry trained, fully background checked professionals available on demand 24/7/365.

PEOPLE
PREMISES
PROCESSES
SYSTEMS
SUPPLIERS

Having a resilient, stable and highly secure cloud solution in place will result in far less support tickets being created and relieve the burden on in-house staff, allowing them to focus on other business priorities. Additionally, once successful migration has been achieved, there will be long-term reduction in capital and operational expenditure, not to mention avoiding the financial and reputational costs or unexpected downtime that could result from an attack or leak of sensitive company data.

CONCLUSION

YOU SHOULD NOW HAVE A BETTER UNDERSTANDING OF HOW TO AVOID BECOMING THE WEAKEST LINK IN THE CYBERSECURITY CHAIN. ADOPTING A ‘SECURITY-FIRST’ MENTALITY AND INSTILLING THIS ATTITUDE INTO EACH MEMBER OF THE WORKFORCE IS THE BEST METHOD FOR PREVENTING ANY FORM OF CYBERATTACK OR DATA BREACH AND ONCE IT BECOMES STANDARDISED PROCEDURE, THE PROBABILITY OF BEING COMPROMISED WILL BE SIGNIFICANTLY REDUCED. TECHNOLOGY IS VITAL FOR PROTECTING DIGITAL INFRASTRUCTURE, BUT CLOUD HOSTING PROVIDERS AND SECURITY COMPANIES ARE SIMPLY OFFERING SERVICES, NOT SOLUTIONS, AND THE SAFEGUARDING OF VALUABLE CORPORATE INFORMATION WILL ALWAYS BE AN INDIVIDUAL’S RESPONSIBILITY, WHETHER THAT PERSON IS THE CLEANER OR A MANAGING DIRECTOR.

THE BUNKER
Ash Radar Station
Marshborough Road
Sandwich
Kent
CT13 0PL

Telephone: 01304 814800
Email: info@thebunker.net

THE BUNKER

Part of the CYBERFORT group

THIS WHITEPAPER WAS PRODUCED BY THE BUNKER AND ITS DEDICATED SECURITY TEAM.

THE BUNKER MD: PHIL BINDLEY

AGENCI MD: GARY HIBBERD

ARCTURUS MD: SIMON FLETCHER

VISIT **THEBUNKER.NET** OR CALL OUR TEAM ON **01304 814800** TO FIND OUT HOW WE CAN HELP YOU WITH YOUR DATA SECURITY.