FORATION

Simply keeping you connected

Guide to Improving your IT Security:

A layered Approach

Foration Whitepaper

February 2015

foration.com | 020 7099 9384 | info@foration.com

Executive Summary

Security Backdrop

With the growing range of security threats and data breaches, protecting your business has never been more important.

A survey by Kaspersky and B2B International revealed that 94% of companies experienced a cyber-attack in 2014. This is 3% higher than the previous year, with businesses of all sizes affected, including SMEs.

Despite these statistics, SMEs are failing to prioritise their IT strategy. A common misconception among smaller businesses is that cyber-criminals are less concerned with companies of their size. In reality, less stringent security controls make them an attractive target. Last year 31% of all cyber-attacks were on SMEs.

A security threat or data breach can prove costly to your business, resulting in:

- Loss of data and intelligence
- Breach of client confidentiality
- System damage
- Increased downtime and reduced productivity
- Reputational damage
- Loss of business

With the estimated cost of a data security breach to a UK SME averaging at £48,000 in damages and reactive spend, ensuring your business is protected is critical.

In this whitepaper, we provide a multi-layered and practical approach to securing your systems. The guide addresses your data and device security, employee education and ongoing management, striking the right balance between flexibility, educational awareness and technical security controls.

> “94% of companies experienced a cyber-attack last year”

Protecting your Data

Email Security

We start this guide by looking at email, which has become the single most important form of information exchange. This tool is critical to your business, but also presents the biggest security threat.

With the growing range of email threats, the reliability and security of your entire system could be at risk with unsecured email. Spam impacts productivity, malware affects network performance and phishing attacks leave your data vulnerable to leaks. Mitigating these risks, without reducing the benefits of email, is essential.

Email management systems integrate seamlessly with your email provider and deliver additional layers of security by;

- Protecting against spam, viruses, malware and malicious links within email content.
- Deploying company-wide email security policies.
- Providing 100% service availability to ensure you are never without email access.
- Retaining a full and secure copy of all emails for legal or regulatory purposes.
- Preventing sensitive information from being transmitted over the internet.

Using a Cloud-based email management platform enables email threats to be blocked before they ever reach your network.

Internet Browsing

To protect against the growing number of internet based threats, we recommend using a web monitoring solution. These are relatively inexpensive and prevent users from inadvertantly accessing malicious websites from links. They can also restrict general website browsing to improve productivity and avoid employee misconduct. Key benefits include:

- Preventing web-based threats from infecting your network.
- Ensuring all web content is free from malicious code.
- Restricting selected sites to boost productivity and comply with company policy.
- Logging all browsing activity.

Securing your web traffic not only protects your business from malware, it improves productivity and protects your bandwith.

Usernames & Passwords

Your systems are only as secure as their weakest link. Typically this is a person's username and password. Recent high-profile iCloud data leaks show that being able to obtain a person's username and password, means you can access all of their data.

To further protect your information, we recommend using two form factor authentication. This relies on entering 'something you know' (username and password – factor 1), with 'something you have' (mobile phone or your location – factor 2).

With two form factor authentication, if you are in an untrusted location when trying to access an email or document, the system requests you to enter a PIN which is sent via SMS to a previously registered mobile device. This means an attacker must compromise both factors to gain access to your data, making a breach far less likely.

Protecting your Devices

Computers

Securing the computers which access and store your company data is as important as securing your data itself. Without this protection, the performance of your network is placed at risk. We recommend a combination of the following:

- Protecting user access through enforcement of password policies and automated account locks in the event of multiple failed logins.
- Protecting against system compromise by preventing the execution of unauthorised, unsecure or untested applications.
- Protecting all local data through full hard drive encryption, preventing unauthorised access in the event a PC being lost or stolen.
- Protecting against data leaks or viruses through the disabling of removable media, such as USB port access.
- Protecting against accidental reconfiguration of system settings by users that could compromise system security.
- Protecting against the latest security threats through anti-virus and anti-malware software.

These controls reduce the failures and slowdowns associated with unmanaged systems, thereby reducing downtime and improving productivity.

Mobile Devices

Mobile phones are now like pocket computers and have the ability to access all of your information. Although this has huge benefits in terms of flexible working and productivity, it introduces an additional threat to your IT security.

We recommend implementing a mobile device management system to ensure that all enrolled devices, whether company or employee owned, are compliant with company security policies. Compliance can include:

- Enforcing complex passcodes
- Enforcing data encryption
- Restricting the geographic location in which a device can or cannot be used
- Preventing the ‘jail breaking’ or installation of certain insecure applications
- Controlling a device's features, such as the use of the camera

In the event of a non-compliance, immediate and automatic remedial action can be taken which includes: alerting IT / management of a compliance violation, disabling the device or completely removing all company data.

Additionally, in the event of a device being lost or stolen, or an employee contract being terminated, company data can be wiped remotely from the device. This targeted removal protects company data, whilst leaving any personal data untouched.

System Administration

Access and User Education

Even with the best security technology in the world, your systems can be left exposed if employees are unaware of risks or fail to understand their responsibilities in safeguarding sensitive data and protecting company resources. Clear policies and regular training are essential to educate employees and enforce the following:

- Limiting the ability of employees to install software on their machines and establishing clear guidelines of what should be saved on company computers.
- Enforcing strong passwords, changing them regularly and keeping them secret.
- Increasing awareness of suspicious links in emails and social media. If there is any doubt, employees should not click on the link!
- Encouraging employees to back up their work, whether automatically or manually.

Training employees is a critical element of security. Employees that understand the value of protecting company information and their role in keeping it safe will be more vigilant and less likely to introduce a threat to your system.

Ongoing Management

24/7 Monitoring and Support

The final peace of the jigsaw puzzle is maintenance and monitoring. This is vital for ensuring the ongoing reliability, security and performance of your systems.

Maintenance should include regular patching, as well as updates to applications and operating systems. Backups should be tested on a daily basis and regular security checks undertaken. According to a recent survey by Cisco, less than 40% of businesses manage patch updates effectively, despite their important role in securing your systems.

This is where a managed service provider can help. Remote management software sends automatic alerts in the event of a patch update or issue, enabling minor issues to be identified and resolved before any business interruption. IT providers that deliver 24/7 support and management can ensure these issues are dealt with as soon as they are detected.

FORATION

Simply keeping you connected

About Foration

Foration delivers smart, tailored IT services to help businesses grow through technology. With expert support, strategy and education, we empower businesses and their employees to work smarter and faster. Service is at the heart of everything we do, which is why we resolve 75% of all requests within 1 hour.

Whether you need IT support and management, business continuity, security or Cloud services, we are on hand to help.

Sources

http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html

http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf

Foration Limited
Somerset House
Strand
London WC2R 1LA

020 7099 9384

www.foration.com
info@foration.com