The Security Mindset

How to keep your business secure with information security

Digital Craftsmen
Email: info@digitalcraftsmen.com
Phone: 020 3745 7706
Twitter: @DCHQ

Table of Contents

Introduction

When someone mentions Information Security, many business leaders switch off.

We're never going to get hacked. It wouldn't happen to us. So why should we spend time and resource on making sure our systems are secure?

But data hacks are on the rise and businesses with sensitive data are increasingly seeing their systems being targeted by malicious parties.

And that's where the security mindset comes in.

Security is not a checklist of programmes to install, applications to set up or people to hire. Security is a culture within organisations. It's a mindset about what you're doing in the cloud.

Security is is all about mitigating risk. When you get started with information security plan, as you might well be starting now, you'll go through and recognise the different types of assets your business holds.

This might be consumer data, financial data, IP or other business critical information.

All of your data and IT resources have a value to malicious third parties and hackers; there are now forums which trade such data and access to it. So you need to put controls in place to manage that risk or vulnerabilities to that information asset.

As you can see, when we talk Information Security, we're talking reducing or mitigating risks to your business assets.

This concept goes across everything you do as a company. For example, when onboarding new hires, you need to take them through understanding Information Security, take them through your company policies, explain what they can and cannot do. Then when people are doing their job and going using your IT systems, you make them think about exactly what they're doing and think about how to be secure.

That's the security mindset.

This whitepaper is designed to help you understand how you can introduce the security mindset to your organisation and dramatically reduce the risk of your company being hacked.

Information Security Basics

Now you have been introduced to the concept of the security mindset, let's take a look at what is information, defining information security, explaining what happens when a company gets hacked and the benefits of maintaining a healthy information security mindset.

What is information?

Organisations of all types and sizes collect, process, store and transmit information in many forms including electronic, physical, verbal and can be intangible.

The value of information goes beyond written words: knowledge, concepts, ideas and brands are examples of intangible forms of information.

> ***"Information is an asset that, like other important business assets, has value to an organisation and so needs to be suitably protected."***

Information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organisation's business and consequently deserve or require protection against various hazards.

Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities.

What is Information Security?

Changes to business processes and systems or other external changes may create new information security risks. Information security risks are therefore always present.

Effective information security reduces these risks by protecting the organisation against threats and vulnerabilities, and then reduces impacts to its assets.

> ***"Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected."***

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisational structures and software and hardware functions.

It is achieved using a combination of suitable strategies and approaches:

- Determining the risks to information and treating them accordingly
- Protecting CIA (Confidentiality, Integrity and Availability)
- Securing people, processes and technology

These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organisation are met.

What are the risks of not adopting a Security Mindset?

If you do not adopt a Security Mindset or have loose Information Security in place, not only will you experience fear, uncertainty and doubt over whether your IT systems are secure, but if you are hacked then there are many more business critical incidents that can happen.

For example, security incidents can cause:

- IT downtime, business interruption
- Financial losses and costs
- Devaluation of intellectual property
- Breaking laws and regulations, leading to prosecutions, fines and penalties
- Reputation and brand damage leading to loss of customer, market,
- Reduced business partner or owners' confidence
- Lost business

What are the benefits of adopting a Security Mindset?

Once you understand the risks, you can see the benefits of adopting a security mindset.

Information security is valuable because it:

- Protects information against various threats
- Ensures business continuity and information security during incidents
- Minimises financial losses and other impacts
- Optimises return on investments
- Creates opportunities to do business safely
- Maintains privacy and compliance

Overall, Information Security gives you more confidence in your IT systems, helps you understand your landscape and where the risks are, and gives you the agility to respond quickly to any attacks

But It's not just about protecting access to data, but making sure it's available to the right people at the right time. With this in mind, Information Security can be defined as the preservation of:

- **Confidentiality:** Making information accessible only to those authorised to use it
- **Integrity:** Safeguarding the accuracy and completeness of information and processing methods
- **Availability:** Ensuring that information is available when required

Now that you know what Information Security is and what you are aiming to preserve, let's take a look at the system Digital Craftsmen adopts to ensure your business is secure.

People, Process and Technology

As we've seen, information security is something you do; it is a process and not a product. Security is all about protecting your information's Confidentiality, Integrity, and Availability

At Digital Craftsmen, we approach Information Security through three key areas: People, Process and Technology.

> ***"Most people just rely on technology, but if you don't have the people in place or the processes it will fail."***

Let's take a closer look at each.

People

People are the biggest weakness when it comes to Information Security. Your biggest threats arise from your staff, yet your biggest asset is your people.

People who use or have an interest in your information security include:

- Shareholders/owners
- Management and staff
- Customers/clients, suppliers and business partners
- Service providers, contractors, consultants and advisors
- Authorities, regulators and judges

Through adopting a Security Mindset, you can implement a culture that's your company benefits. Putting them on training courses, taking them through policies and making them aware of what they should and shouldn't be doing are all key steps.

After they've had training and adopt the Security Mindset, everyone will now be thinking with security in mind - "If I'm doing something, what is the process, what is the risk?"

It's about giving people the security mindset and awareness of how they can be secure.

Process

Processes are work practices or workflows, the steps or activities needed to accomplish business objectives:

Processes are described in procedures.

Virtually all business processes involve and/or depend on information this makes information a critical business asset.

Information security policies and procedures define how we secure information appropriately and repeatedly.

When you work with Digital Craftsmen, we put an Information Security management system in place which manages the whole lifecycle of risk.

Part of that is the requirement to have procedure in place to dictate certain areas, such as project management, change management, incident management.

For example, we'll put in place dedicated roles for dedicated people who can investigate and update when issues are fixed. So if you get attacked by hackers, we can be confident of the process in place so everyone knows exactly what they need to do.

By having an Information Security process in place, you can also have alerts and responses set up so your team can resolve any issues and get back everything back up and running, ensuring that a client's corporate reputation is not affected.

This is bigger benefit is of following the security mindset - with a clear of set of roles, you can be more agile and have a faster response to any attacks on you systems.. If something does happen then you're reducing downtime and saving costs.

Technology

Technology security covers a lot - from VPNs to managed firewalls, from log analysis to locking down dev environments, from patching to directory services.

Here’s a checklist of the areas technology covers in Information Security:

Information technologies:

- Cabling, data/voice networks and equipment
- Telecommunications services (PABX, VoIP, ISDN, videoconferencing)
- Phones, mobile phones and devices
- Computer servers, desktops and associated data storage devices (disks,
- tapes)
- Operating system and application software
- Paperwork, files
- Pens, ink

Security technologies:

- Locks
- Entry Barriers
- Card-access systems
- CCTV

There are also industry alerts and vulnerabilities around different tech that are frequently published online. You need to be making sure you have a process in place to assess the risks of new vulnerabilities quickly, then address or mitigate the risk. After assessment you can downgrade some risks to a lower priority based on your exposure resources and security stance. Critical Risks that cannot be addressed in house can be transferred to a specialist providers such as Digital Craftsmen.

Information Security Best Practices

Security-firm Fallible created an online tool to reverse engineer any android app to look for secrets and keys to AWS accounts. These keys and secrets can give full and uncontrolled access to extract and delete entire customer data sets and all the machines that go with them to run your application and site.

Fallible built the tool because of an internal need, as the company were constantly required to reverse engineer apps for their customers to examine them from a security standpoint.

The company have now reverse engineered over 16,000 apps and found that although most of the apps didn't have any sort of key or secret in the app, they reported that "some 2,500 apps contained either secrets or third party keys". That's a big security risk to those apps and – ultimately – to the user.

Fallible's findings show that lots of developers are indeed "fallible" and aren't so good at setting up a secure infrastructure or enforcing security and separation and best practices.

How to secure online products and services

So what lessons can you learn from this to make sure your products and services are secure?

The key for developers to make sure their products and services are secure is by following security best practices. But the honest answer is that unless you are a professional systems administrator you are unlikely to know such best practices.

Here are some of the common methods that developers can use to secure their products and services:

1. Separation of concerns: Running servers and services on isolated or separate Virtual Machines or containers. Understand where your critical data is stored, and use firewalls and Access Control Lists to limit traffic to and from those network segments.

2. Password policies: To strengthen and clarify the education given to your users, you should clearly outline the requirements for using strong passwords. Make sure employment contracts and SLAs have sections that clearly define these security requirements and that your team are using strong passwords.

3. Limit permissions granted: Only allow the tool or user to do the bare minimum or what they require. By creating specific controls for all of your users, you limit their access to only the tools and systems they need to do their job or perform a task.

4. Encryption: Encrypt everywhere possible, such as in transit, at rest, within code and on your versioning system, etc. Encryption is essential to protecting sensitive data and to help prevent data loss due to theft or equipment loss.

5. Implement user activity monitoring: This allows you to monitor users and see what they are doing on your system and provides an audit trail. If a malicious user gains access to an employee's system – or if an insider chooses to take advantage of their system access – you will be notified of any suspicious activity

6. Patch any security holes: Despite the hype, most hackers exploit known vulnerabilities. Make sure you are investing time in patching your systems and keeping up to date with the latest developments in the security world.

7. Automate: Your attackers are using automated tools to scan ports and identify misconfigured devices, so you should be automating your system security. Automating security tasks not only mitigates human errors, but frees up precious developer time to focus on more strategic initiatives.

8. Educate your users: Have a well-organised, well-understood, well-maintained, and well-monitored security policy for both employees and third-parties that access your system. Also make sure they undergo periodic training to keep their understanding of security policies up to date.

9. Avoid hard coding: Never hard code plain text secrets or keys into your source code!

How to secure cloud services like AWS and Azure

To add more complexity into the mix, each cloud service or provider also has a 'best security practices' guide – potentially for each service they provide.

For example, Amazon Web Services' (AWS) security best practices guide provides security best practices that will help you define your Information Security Management System (ISMS) and build a set of security policies and processes for your organisation so you can protect your data and assets in the AWS Cloud.

Their guide also provides an overview of different security topics such as identifying, categorising and protecting your assets on AWS, managing access to AWS resources using accounts, users and groups and suggesting ways you can secure your data, your operating systems and applications and overall infrastructure in the cloud.

Likewise, Microsoft Azure have a security best practices and patterns guide, derived from their experience with Azure networking and the experiences of managed cloud services specialists like Digital Craftsmen.

How to make sure your IT systems are secure

The main point to keep in mind is that security is an ongoing concern. You need to adopt a Security Mindset.

Although computing is on-demand and developers now revel in the flexibility they have to provision machines, they may not have the skill set or time to manage your production systems or the ongoing operation of your new system.

The security landscape is changing rapidly, which means you need to allocate resource to managing security and implementing best practice. If you do not have the expertise or resources to devote to IT security or system planning, you should consider transferring this risk to a specialist managed cloud provider such as Digital Craftsmen.

Conclusion

If you want to discuss the security of your cloud product and services, then Digital Craftsmen are the right people to speak to.

We're managed cloud specialists who are ISO 27001 accredited and have been securing client's online products and services with security best practices and an ITIL service desk over 15 years.

We understand the risks and everything we can put in place mitigates that risk for your business. We have the skills and experience to make your cloud setup secure.

Here is a full list of Information Security services we offer:

- Security Review: Undertake review of client security preparedness
- Penetration testing: Facilitate 3rd party penetration tests
- PCI Readiness: Self-assessment audits for PCI compliance
- Secure VPN: Adding security and privacy to private networks and the sharing of data over public networks.
- Managed Firewall: Initial access is limited to only web traffic and any changes to firewalls are strictly controlled by your approved authorisers
- Operating System Patching: Monitoring of industry alerts for operating system patches and application in our planned maintenance schedule
- Middleware Patching: Monitoring of industry alerts for key middleware components like web servers, application engines and programming languages and applying in our planned maintenance schedule
- Anti-virus: Managed anti-virus platform
- User Management: Access control across multiple platforms and applications
- Certificate and Key Management: Deployment of PKI infrastructure on Windows and Linux
- Directory Services: Central to the security design of an IT system and generally have a fine granularity of access control

Every service we offer follows this security mindset and the processes we have in place.

If you need an assessment of where you stand over Information Security, call Digital Craftsmen now on 020 3745 7706 or email info@digitalcraftsmen.com for more information on our Information Security services.

Contact Digital Craftsmen

Digital Craftsmen can offer strategic automation design for your current cloud services set up. We can help you plan an automation strategy and – if you have no automation today – we can help you implement automation throughout your organisation.

Speak to an expert today:

Digital Craftsmen
Email: info@digitalcraftsmen.com
Phone: 020 3745 7706