Executive Briefing Guide

In association with

Managing Web and Mobile Security Risk

An introduction to continuous assessment for business executives

March 2017

In a nutshell

The chances are that your organisation is becoming increasingly dependent on digital channels. This in turn shines a spotlight on the importance of securing the applications and services that underpin your online and mobile presence. Achieving this while your developers are releasing new and updated software frequently can be a challenge, especially when cyber criminals are getting smarter by the day. Against this background, a more continuous approach to security assessment is key.

Authorities are introducing ever stronger regulations, and the penalties that accompany these can be substantial.

Purpose of this guide

The topic of cyber security can be frightening to think about, and it's not just the news stories of embarrassing and damaging data breaches, and the worry that something similar might happen to you. Governments and other authorities are introducing ever stronger regulations around areas such as privacy, and the penalties that accompany these can be substantial.

Against this background, you undoubtedly appreciate the need for cyber security, and know that ultimate responsibility lies with the officers of the company should anything go wrong. Yet as a senior business manager or executive yourself, you don't have either the time or the expertise to delve into the practicalities. This makes it hard to have a conversation with your IT or security team about how well risks are being managed. It's also challenging to answer the critical question - "Are we secure?" - with any meaningful level of confidence.

If any of this sounds even partly familiar, then this short non-technical guide is for you. Our aim is to arm you with insights into how risks are assessed in relation to the security of your website, any mobile applications published by your organisation, and the software that makes it all work.

Digital channels have become fundamental to most businesses.

Putting the discussion into perspective

A good place to start with the discussion around web and mobile security is to remind ourselves just how fundamental digital channels have become to most businesses. The results of a recent international survey of 1,442 organisations, for example, tell us that already around 7 in 10 regard the web and mobile technology as either critical or important for effective customer engagement (Figure 1).

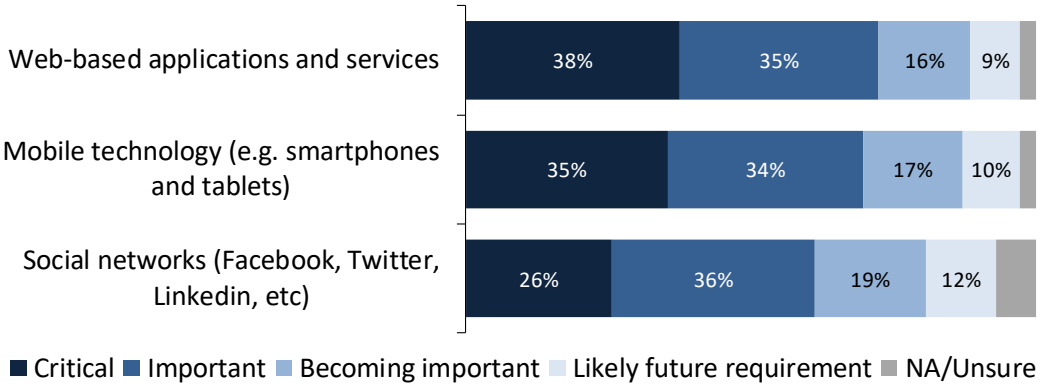


Figure 1
Importance of digital channels for customer engagement

Source: Freeform Dynamics
International survey conducted 2015
1,442 IT and business professionals

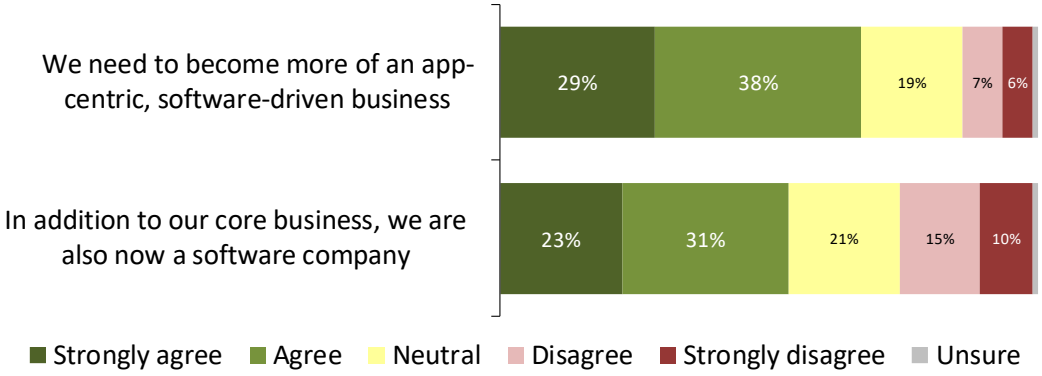
It's also notable from the above chart that regardless of the current level of importance cited, almost all of those surveyed acknowledged the growing or future role of digital channels. It would be surprising if your organisation was any different.

Business is nowadays enabled by software.

In order to enable this digital activity you need various forms of software - the web applications and mobile apps with which customers interact, connected into your core business systems as appropriate. It therefore makes sense that in the same research study, two thirds of respondents strongly agreed or agreed with the notion that they need to become more of an app centric, software driven business (Figure 2).

Figure 2
Importance of software to the business

Source: Freeform Dynamics
International survey conducted 2015
1,442 IT and business professionals

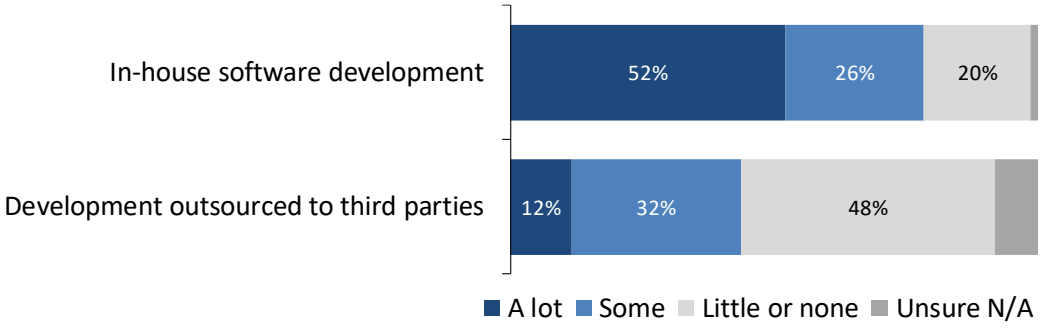


A lot of the software you need to deliver a well-differentiated online presence has to be developed and/or customised.

As we can see, over half of those participating in the study also indicated that in addition to their core business, their organisation could now be thought of as a software company too. The reason for this is because off-the-shelf packages such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and commercially available marketing solutions might be important for digital business, but in themselves they are rarely enough. A lot of the software you need to deliver a well-differentiated online presence and effective digital experience to customers has to be developed and/or customised to meet your specific requirements. The chances are therefore that you have one or more teams designing and building software in-house and/or via contract or outsource arrangements (Figure 3).

Figure 3
Level of custom software development undertaken or commissioned

Source: Freeform Dynamics
International survey conducted 2016
2,038 IT and business professionals



The need is to ensure that software cannot be hacked, brought down or otherwise abused by criminals looking to damage your business or steal your data.

Pulling all this together we can summarise by saying that an effective digital/online presence is key to business success nowadays, which in turn means your organisation has a lot of software connected over the internet to the outside world, and this online presence is set to grow. When we talk about web and mobile security, we are referring to the need to ensure that this software cannot be hacked, brought down or otherwise abused by criminals looking to damage your business or steal your data.

Security starts with protecting your network

If you ask your IT or security team what measures have been put in place to ensure that your website and other digital channels are secure, they are likely to highlight a range of tools and techniques. Firstly, for example, they'll talk about firewalls and other barriers to block illegitimate or suspicious incoming requests to access your

network and the systems that run on it. They may also allude to various early warning and response mechanisms to identify when your network has been breached so that cyber attacks can be detected and neutralised as quickly as possible.

No security measure is ever fool-proof, so it's very common, indeed highly recommended, to blend different types of technologies and services.

If you hear about multiple types of protection when you inquire what's in place, rest assured there's a good reason for this. No security measure is ever fool-proof, so it's very common, indeed highly recommended, to blend different types of technologies and services. The fact that these sometimes overlap is not a waste of money. The principle at work here is that even if an attack defeats or evades one of your protection measures, it will be picked up by one of the others. Of course there are no absolute guarantees, because just like any other form of risk management, security is a game of probability. The aim is to stack the odds in your favour.

That said, even the most thorough set of 'network level' security measures won't protect you if your applications themselves are open to abuse.

Web application security is a whole other ball-game

Many cyber threats nowadays operate at an 'application level'.

Many cyber threats nowadays operate at an 'application level'. In simple terms, an attack of this kind comes in the form of a request that to the network looks perfectly legitimate - e.g. it could appear as if a normal customer had just filled out a web form and pressed the 'submit' button. Your firewall and other network level security mechanisms therefore wave it through without so much as a warning. What they don't know is that the attacker is looking to exploit a flaw in the application software itself that allows unauthorised access to data, or some other form of misuse or abuse.

Such flaws, or 'vulnerabilities' as they are often referred to in the security world, can be introduced into your environment in various ways. Commercial software products used within your systems can be a common source of vulnerabilities. This is why your IT team has to 'patch' (update) such software, in the same way as security patches have to be regularly applied to your Windows desktop or laptop.

Vulnerabilities can arise from developers making mistakes, or introducing flaws because they don't know any better.

The other way in which vulnerabilities find their way into systems is through application developers making mistakes, or introducing flaws because they don't know any better (e.g. due to inadequate training or lack of awareness).

Whatever the origin of software vulnerabilities, the aim is to prevent, identify and fix them as early as possible. A number of approaches are used here, again on the basis that none of them are fool-proof. Some of the main techniques include:

Whatever the origin of software vulnerabilities, the aim is to prevent, identify and fix them as early as possible.

Development best practices
Definition of the do's and don'ts of designing and building applications securely

Development team training
Making sure development staff have the necessary knowledge and skills

Code scanning
Use of tools that scan developer code to highlight potential vulnerabilities

Pre-deployment testing
Tests at various stages to identify security-issues before the software goes live

Live penetration tests
Use of 'friendly' hackers that spot issues by trying to break into your live systems

The last of those techniques, penetration testing, works on the principle that it's better to hack yourself and fix the problems you identify, than wait for someone else to hack you, and only find out about vulnerabilities after they have been exploited. In many ways you can regard such 'pen testing' (as it's known in security circles) as the final check to make sure everything is as secure as it should be.

It's better to hack yourself and fix the problems you identify, than wait for someone to hack you.

Practical challenges that complicate matters

So far, so good; we have covered the need for network level security as a first line of defence against intrusion by cyber criminals. We have also discussed the role of application level security measures to minimise the chances of vulnerabilities finding their way into the software that underpins your website and mobile apps. If you want to go into more detail, you'll find lots of additional information on the web, but you should now at least have a good feel for the essentials from what we have covered.

Nothing stands still for very long in the web and mobile space.

To complete our discussion, however, there is an important aspect to web application security that we need to touch on. This stems from the fact that nothing stands still for very long in the web and mobile space. On one side of the equation, the way in which your business needs continue to evolve leads to a constant stream of new and updated applications. Meanwhile, the activity of cyber criminals, which is often very well-funded, also continues to evolve, so the 'threat landscape' (as security specialists call it) is literally changing from one day to the next (Figure 4).

Figure 4
Constantly changing applications and threats

Given these dynamics, it's important to appreciate that security is not an end state that you can strive for and reach, and then relax. If you regard yourself to be secure today, that's no guarantee of being safe tomorrow unless you take active steps to keep up with what's changed in the interim. The most useful way to think of web application security is therefore as a continuous process with no finish line.

Security is not an end state that you can strive for and reach, and then relax.

In practical terms, there are some things to consider against this continuously changing backdrop. For one thing, any level of confidence stemming from periodic checking, e.g. monthly or quarterly penetration tests, or intense pre-release testing exercises, can only be short lived, even if the findings reveal an acceptable level of security at the time the tests were conducted.

There is then the issue that many types of testing, including code scanning and pre-production checks (as well as pen tests), often throw up a very large number of potential vulnerabilities. At first sight this may seem beneficial - better to be safe than sorry. Working through all these and prioritising them can be both difficult and resource intensive, however. And if vulnerability assessment isn't effective, your staff end up wasting time on things that don't matter, while major exposures linger.

If vulnerability assessment isn't effective, your staff end up wasting time on things that don't matter, while major exposures linger.

The danger is that your staff end up spending so much time testing that they've little left over to do useful, productive work.

Dealing with these challenges has traditionally not been that easy. One option is to allocate lots of in-house resources to the problem and instigate a programme of continuous intensive testing using the tools available to your IT or security team. The danger is that your staff end up spending so much time testing that they've little left over to do useful, productive work.

Another option might be to increase the frequency of penetration testing. The problem here is that such an approach would be prohibitively expensive, as services in this area tend to be priced on a consulting basis.

Another way to go is the outsourcing route.

Continuous security assessment services

We have seen the emergence of service offerings that allow continuous security assessment to be achieved through outsourcing.

In order to deal with some of the practical challenges mentioned above, we have seen the emergence of service offerings that allow continuous security assessment to be achieved through outsourcing. The providers in this space differ from traditional pen testing companies in that they exploit economies of scale to centralise and reuse much of what's involved in the intelligent assessment of risk on an ongoing basis.

It is beyond the scope of this document to go into a lot of detail here, but the essentials of such services are as follows:

- Powerful tools running in the provider's data centre simulate the actions of cyber criminals looking to exploit application level vulnerabilities. These can be used to assess the security of your websites and mobile applications according to any schedule set by your IT or security team - continuously if that's what's required.
- Potential vulnerabilities discovered during this testing process are assessed and prioritised using global threat intelligence data. Any new or different issues that emerge are checked by an experienced analyst, and validated individually. This ensures that your staff are not distracted by a large number of 'false positives'.

Security index ratings are derived from data such as the number of vulnerabilities, their level of severity, and the rate at which issues are being fixed.

- Vulnerabilities are reported back to your internal team in an actionable format so they can get on and address what's most important from a real-world risk perspective. The service provider will often go beyond just flagging up an issue, and suggest an appropriate fix based on hard-intelligence and best practice.
- A good service provider will also generate an overall security index rating for each of your websites and applications. These index ratings are derived from data such as the number of vulnerabilities, their level of severity, and the rate at which issues are being fixed. This in turn allows benchmarking against industry averages.

This last aspect of the type of service we are talking about here is particularly useful for assessing both your current level of vulnerability and the effectiveness of your ongoing security management process.

The beauty of the index-based approach is that you don't have to understand the specific technical detail.

The beauty of the index-based approach is that you don't have to understand the specific technical detail to participate in discussions around the health and performance of the organisation from a security perspective. This means you can more easily engage with your IT or security team to review risks, prioritise remedial efforts and allocate any funding necessary to drive improvement. Another big benefit is that you can monitor index scores over time. This enables you to track the positive impact of your investments, or conversely, the negative impact or drift resulting from either external developments or internal activity.

The bottom line

Continuous security assessment services allow you to manage application security as an integral part of your overall business risk management strategy.

As you continue with your digital transformation strategy, it's important to regard cyber security as a fundamental aspect of business risk management, taking care of web application security as part of this.

Given the constantly changing nature of both your software portfolio and the threat landscape, the key is to think in terms of implementing a web application security management process. Just like any other form of process, this then opens the door to outsourcing in order to boost efficiency and achieve a better overall outcome for the business. This is where continuous security assessment services come into their own.

Such services are by no means a magic bullet, but used together with the other measures we have highlighted, they can both increase your overall level of security, while at the same time freeing up skilled staff to focus on more productive activities. Perhaps most importantly, however, they provide you with the insights and visibility you need to manage application security as an integral part of your overall business risk management strategy.

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we aim to help busy IT and business professionals get up to speed on the latest technology developments, and make better-informed investment decisions.

For more information, and access to our library of free research, please visit www.freeformdynamics.com.

About WhiteHat Security

WhiteHat Security has been in the business of securing web applications for 15 years. Combining advanced technology with the expertise of its global Threat Research Center (TRC) team, WhiteHat delivers application security solutions that reduce risk, reduce cost and accelerate the deployment of secure applications and web sites. The company's flagship product, WhiteHat Sentinel, is a software-as-a-service platform providing dynamic application security testing (DAST), static application security testing (SAST), and mobile application security assessments. The company is headquartered in Santa Clara, Calif., with regional offices across the U.S. and Europe.

Terms of Use