FREEFORM DYNAMICS

Inside Track Research Note

In association with

WhiteHat SECURITY

# Cyber Security Ownership and Responsibility

## A guide for senior business executives

February 2016

# In a nutshell

**It's easy to be caught out by a cyber attack or internal mistake that leads to your customers' data or important intellectual property ending up on the black market. Making sure your business is adequately protected and is able to respond effectively to a security incident is a main board matter. A fundamental imperative for your executive team is therefore to address the question of ownership and responsibility.**

> *Making sure your business is adequately protected and is able to respond effectively to a security incident is a main board matter.*

# Business as usual; got it covered

In the unfortunate event that a problem occurs in your core business, the chances are that it will be spotted and acted upon quickly. If a supplier lets you down, for example, whoever is responsible for the relationship or transaction might simply switch to an alternative source of goods or services. If the price goes up as a result, approval of the switch will be sought from the relevant manager. If delays in delivery are anticipated, the right people will be notified to allow adjustment of production schedules, resetting of customer delivery expectations, or whatever else is necessary. Your business is organised to take such things in its stride.

> *In the unfortunate event that a problem occurs in your core business, the chances are that it will be spotted and acted upon quickly.*

Key to making this work is a clear understanding of who is responsible for what as your business goes about its core activities. People know what's expected of them and who to go to when a particular event occurs or an exception arises. Even if prevention, monitoring, contingency and escalation arrangements are not exhaustive, which is usually the case in the real world, the chances are your people will have things covered. Sure, stuff sometimes falls through the cracks, but unless you have a particularly unhealthy culture of fear which encourages problems to be hidden, 'situations' will soon be flagged up to senior management.

# Cyber security as usual; too easily caught out

> *Things often work differently in relation to the security of your IT systems.*

Things often work differently in relation to the security of your IT systems and electronic data. The news stories featuring interviews with harried-looking senior executives or communications officers provide a clear illustration of this. All too often, a cyber security breach turns into a huge crisis overnight, leading to reputational damage, loss of customer confidence and even legal exposure. Yesterday things were fine, today they are falling apart and everyone seems to be surprised and floundering. Spokespeople are evading or stumbling over straightforward questions about what happened and why, and, more importantly, what's being done about it.

> *All too often, a cyber security breach turns into a huge crisis.*

Of course depending on the nature and profile of your business, this kind of crisis may or may not hit the six o'clock news. Either way, potentially embarrassing calls and letters to customers and regulators are inevitable - indeed it will often be a regulatory requirement - meaning your reputation, top line and bottom line can still be hit hard.

> *A mistake often made is to assume that the answer is to delegate the responsibility of protecting your organisation to the IT team.*

To be fair, many business executives nowadays appreciate the cyber security imperative, and the fact that you are reading this document means you are likely to be one of these. However, a mistake often made is to assume that the answer is to delegate the responsibility of protecting your organisation to the IT team, on the basis that they understand the technicalities. While specific security expertise is important, however, we can consider this to be 'necessary but insufficient'. The truth is that cyber security is first and foremost a business issue, so it must be approached in that way. Do this and you will minimise the risk of nasty surprises.

> *Cyber security is first and foremost a business issue.*

# Understanding the nature of the game

One of the challenges in this area is that cyber security specialists often seem to speak a different language to the rest of us. Fortunately, you don't need to know what most of the buzz words and acronyms mean. There are a handful, though, that are useful to help you understand some fundamental principles that are key to elevating the discussion to a business level in a practical and actionable manner:

*One of the challenges in this area is that cyber security specialists often seem to speak a different language to the rest of us.*

Table 1: SOME KEY CYBER SECURITY CONCEPTS

| *Term* | *Meaning* | *Significance* |
|---|---|---|
| External threat | You can think of this as a source of risk from the outside world. Criminal organisations looking to steal your customers' data for selling on the black market is an example here, as are groups looking to cause damage or get attention for political reasons. | Your organisation needs to be aware of the threats that exist and the methods employed by the so-called 'Black Hats', so you can put the necessary defences in place. |
| Internal threat | Threats can also exist within your organisation. Obvious examples here include disgruntled or dishonest employees. Less sinister but equally threatening are ill-informed or careless employees who are more prone to making damaging mistakes. | Protection is needed here, not just to deal with internal threats per se, but also because external attackers will often try to use your employees as a route into your systems. |
| Vulnerability | As the term suggests, we are talking here about weaknesses or gaps in your systems or protection measures. Examples range from computers not being properly updated, through flaws in business software, to simply users relying on weak passwords. | Vulnerabilities can be exploited to gain unauthorised access into your systems and data. Some can also increase the chances of mistakes being made or accidents happening. |
| Attack or incident | Against the backdrop of the kind of threats we have highlighted, it is inevitable that your systems will be attacked and/or incidents will occur as a result of accident or mishap. We can think of these as threats materialising as tangible events. | Security events such as these may or may not lead to loss or damage. If you are vigilant and have the right protection in place, attacks can be blocked and incidents neutralised. |
| Security breach | Some attacks and incidents will lead to your systems being penetrated and/or data ending up in the wrong hands. Such breaches are ultimately what you are trying to prevent, but it's important to appreciate that nowadays they are inevitable. | You must assume that at some point your protection will fail. The imperative is to plan for this so you can react quickly to both minimise the damage and manage the consequences. |

*Your organisation needs to be aware of the threats that exist and the methods employed by the so-called 'black hats', so you can put the necessary defences in place.*

*External attackers will often try to use your employees as a route into your systems.*

*You must assume that at some point your protection will fail. The imperative is to plan for this so you can react quickly to both minimise the damage and manage the consequences.*

Pulling all this together, from a business perspective, the game is about:

- Understanding the threats and vulnerabilities that lead to exposure
- Blocking attacks and preventing security breaches as well as you can
- Reacting quickly and effectively when a breach inevitably occurs

Even though you probably don't want to (and definitely don't need to) understand the technicalities, it's pretty easy to appreciate the logic behind these imperatives. And the good news is that there are lots of skills, technology solutions and best practices that can be brought to bear in each of these three areas. Why, then, are so many organisations still caught out by cyber security breaches that with the benefit of hindsight could easily have been prevented?

# Acting on the imperatives; an executive view

As a senior business manager, it is tempting to just delegate the cyber security problem to the IT department, and let them work out what to do about it within their existing budget and resource constraints. However, the hands-off approach is undoubtedly a major contributor to executives ending up squirming in front of the cameras. You need to take an active interest for a number of reasons:

*The hands-off approach is undoubtedly a major contributor to executives ending up squirming in front of the cameras.*

- Cyber security is a business issue, and the main board is ultimately accountable
- The threats are real and will damage your business unless you take precautions
- Implementing protection and response measures takes time, effort and funding
- Everyone in the business has a role to play, and business leadership is required

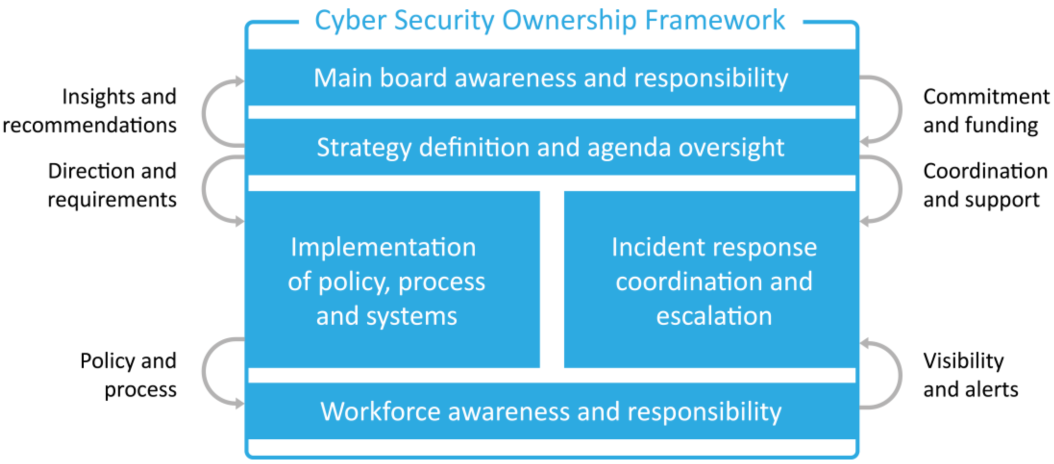
None of these points are up for debate, and we make no apologies for any discomfort we may have caused by listing them in this simple, matter-of-fact manner. But if you know or suspect that cyber security has been neglected in your organisation, or at least hasn't been given the attention and resources it deserves, the answer isn't to start issuing directives or even throwing money at the problem. It's first and foremost about making sure you are properly organised, and coming back to where we started, the foundation is a clear definition of who is going to look after what.

*The answer isn't to start issuing directives or even throwing money at the problem.*

*The foundation is a clear definition of who is going to look after what.*

# The ownership and responsibility framework

A good way of looking at what needs to be done is to focus on ownership and responsibility in 5 key areas (Figure 1).



Cyber Security Ownership Framework
Main board awareness and responsibility
Strategy definition and agenda oversight
Implementation of policy, process and systems
Incident response coordination and escalation
Workforce awareness and responsibility
Insights and recommendations
Direction and requirements
Policy and process
Commitment and funding
Coordination and support
Visibility and alerts

*Figure 1*
The ownership and responsibility framework helps you to focus on what needs to covered

Whether it's the one laid out here, or something similar, if you work to an ownership framework you are much less likely to get caught out. It reduces the chances of simple protection measures being overlooked, or the company becoming exposed as a result of everyone assuming someone else was taking care of something vital.

*If you work to an ownership framework you are much less likely to get caught out.*

The framework shown above presents a top level view. Each of the elements can be broken out into further detail, but as you assign ownership in each of the key areas, the task of dealing with the next level down can be delegated.

# Putting the framework into practice

While we obviously can't be exhaustive on the detail in this short document, we can provide you with a flavour of some of the main practicalities to consider. Let's walk through the elements of the framework and highlight some essentials.

## Main board awareness and responsibility

*Directors have to be up to speed on the nature of the risks and must explicitly assume ultimate accountability for dealing with them.*

Cyber security needs to be a main board agenda item. Directors have to be up to speed on the nature of the risks and must explicitly assume ultimate accountability for dealing with them. This doesn't involve becoming a security expert, but it does mean being tuned into important questions such as *"How much would our business be damaged if our customer data or intellectual property ended up on the black market?"*, *"What would be the cost of our business being offline for an hour, two hours, four hours, etc as a result of a cyber attack?"*, and, not least, *"How would we respond in the face of a major security breach?"*.

Considering questions like these allows you to prioritise requirements and consider funding, resourcing and urgency levels on an objective basis. A key mind-focusing principle here is that when you say 'no' to a security-related investment request, or decline to get involved in key discussions, you are responsible for the consequences, and ignorance is no excuse for lack of involvement, air cover, investment or action.

## Strategy definition and agenda oversight

*Ownership of the strategy and agenda can lie with a single individual who coordinates input and advice from those with the necessary knowledge and expertise. It could equally fall to a multi-disciplinary body.*

Ensuring that the main board is properly briefed and considering the right questions and options brings us onto the importance of defining a strategy and setting out a clear agenda. Ownership of the strategy and agenda can lie with a single individual who coordinates input and advice from those with the necessary knowledge and expertise. It could equally fall to a multi-disciplinary body or team within which decisions and recommendations are made collectively.

Either way, whoever is responsible essentially owns the cyber security agenda. To act effectively, they therefore need to identify and characterise the risks from both a business and practical perspective, then determine requirements for policies, systems and processes. The focus here is on 'what' needs to be addressed and implemented rather than 'how', though in order to advise executives, at least a high level assessment of cost and commercial impact needs to be made where necessary.

*In the absence of an individual or team explicitly owning this part of the framework, you can end up wasting time and money on things that don't matter that much, while neglecting areas that do.*

In the absence of an individual or team explicitly owning this part of the framework, you can end up wasting time and money on things that don't matter that much, while neglecting areas that do. You'll also suffer more from things falling through the cracks.

## Implementation of policy, process and systems

*Clarity is required on who is responsible for specific policies, processes and systems across the organisation.*

From an implementation perspective, clarity is required on who is responsible for specific policies, processes and systems across the organisation. This includes fleshing out requirements, putting whatever is necessary in place, then operating and managing things thereafter.

We could have broken out the IT department from other parts of the business when considering this part of the framework, but while the activities are different, the basic principles of clearly defined ownership and responsibility for the day-to-day aspects of security management are the same.

Within IT, there will be a lot of focus on technology-enabled protection of infrastructure and end-user equipment such as PCs, Macs and mobile devices. Another important area will deal with the measures needed to ensure that software is developed and deployed in a secure manner. An often overlooked requirement is the ongoing monitoring and testing of live systems to ensure they remain secure. This is important because the aforementioned 'Black Hats' are constantly inventing new ways to attack your website and penetrate your network. What was safe last week therefore might not be so secure today.

*Within IT, there will be a lot of focus on technology-enabled protection.*

*An often overlooked requirement is the ongoing monitoring and testing of live systems to ensure they remain secure.*

Within the business, responsibility needs to be defined in relation to the security aspects of standard operating procedures. Wherever possible, security will be an inherent part of day-to-day processes and behaviour, but if you take this approach, the risk is that the safeguards necessary to protect information and assets fall by the wayside when people are under pressure or forget why certain steps in procedures are there. Consequently, there is an imperative for business unit managers, team leaders, supervisors and so on to be made explicitly accountable for the secure operation of their parts of the organisation.

*There is an imperative for business unit managers, team leaders, supervisors and so on to be made explicitly accountable.*

## Workforce awareness and responsibility

Going hand-in-hand with business manager accountability is a need for individual employees to take responsibility for their own actions. This in turn means they need to be given guidance on security risks and made aware of what's expected of them in terms of safe and secure behaviour. Assuming this prerequisite is dealt with, it is right and proper for employees to be held responsible for their own actions. This may even be to the point where particularly irresponsible behaviour is regarded as a disciplinary offence and documented as such.

*Going hand-in-hand with business manager accountability is a need for individual employees to take responsibility for their own actions.*

In terms of specifics, responsibilities such as adherence to explicitly defined security policies and procedures, the dos and don'ts of handling sensitive information, how to prevent unauthorised use of passwords, etc, are pretty straightforward to define (with the help of the IT team). But it is essential to ensure everyone understands why these policies and procedures are in place, and this may well require ongoing education and refreshers.

In other areas, taking a black and white approach can be harder. Examples here include the use of personal equipment for business purposes (and vice versa), accessing public networks while out and about, avoiding 'over the shoulder' viewing of sensitive information on laptop or tablet screens while in public places, and so on. Areas such as these, along with more obvious but frequently overlooked risks like 'autocomplete' errors leading to emails being sent to the wrong recipient, and careless use of USB sticks and SD cards, are where you need to put more of an emphasis on education, awareness and insight rather than hard and fast rules.

## Incident response coordination and escalation

No matter how comprehensive your cyber security measures, you must assume that a breach or major incident will occur at some point and be appropriately prepared. Various processes and actions might be put into place, but one of the most important and effective things you can do is be clear on who assumes ownership of each aspect of managing the response when an incident happens.

*One of the most important and effective things you can do is be clear on who assumes ownership of each aspect of managing the response when an incident happens.*

The best way of thinking of this is to consider the imperatives for each business function or discipline. The IT team, for example, will normally be called on to figure out the nature and extent of a breach, and determine what has been accessed or tampered with. Someone needs to coordinate this, possibly with the help of external resources, then initiate measures to block further loss or damage, and restore normal services. Points of escalation and lines of communication, ultimately to the main board if necessary, must be defined in advance.

*Points of escalation and lines of communication, ultimately to the main board if necessary, must be defined in advance.*

For significant breaches, or those involving loss of information subject to a legal duty of care, it has to be clear who will be involved in making decisions around customer and regulator notification. It's also wise to consider how you will handle news of the incident leaking out, and who will take care of messaging to customers and the media in response to incoming enquiries. The point of all this is to avoid matters getting out of hand and an incident turning into a crisis because no one knows who to turn to for what, and which information needs to be communicated to whom.

## Web security highlights the challenges and imperatives

*If your organisation is keeping pace with industry trends, the chances are that your website has become a critical part of your business.*

So far our discussion has been deliberately generic as it is important to understand the basic principles and imperatives that apply universally. What these translate to in practice, however, varies depending on the specific aspect of cyber security you are considering. Let's therefore take a look at an example of applying the ownership framework in one of the hottest areas that exists at the moment - web security.

If your organisation is keeping pace with industry trends, the chances are that your website has become a critical part of your business, and its importance is continuing to grow. Going hand-in-hand with an effective online presence is integration of your website with your core business systems in order to drive both efficiency and customer responsiveness through various types of automation and self-service capability. From a security perspective, your website becomes a potential route into your network and data for cyber criminals.

*From a security perspective, your website becomes a potential route into your network and data for cyber criminals.*

### The complex and ever-changing 'threat landscape'

Colloquially, the term 'hacking' is often used in the context of web security threats, but the reality is that the Black Hats employ all kinds of mechanisms to penetrate websites that are vulnerable.

Some of the terms you might hear in this area include:

- Cross-site scripting (XSS)
- SQL injection
- PHP/JavaScript code injection
- Arbitrary code execution
- Data breach
- Buffer overflow
- Hidden iframes
- Third party vulnerabilities (click through ads from agencies, etc)
- Cross site request forgery (CSRF/XSRF)

*Asking your IT team to give you a quick overview of the types of risk that threaten your business would be a good excuse to get the conversation going with them in this space.*

If you want to know what these mean, asking your IT team to give you a quick overview of the types of risk that threaten your business would be a good excuse to get the conversation going with them in this space. In the meantime it's worth noting that the list presented is of categories, and that many specific threats exist within each (e.g. there are lots of potential ways of attacking your website via SQL injection). Furthermore, cyber criminals are constantly probing for new vulnerabilities and developing their methods of attack.

*Cyber criminals are constantly probing for new vulnerabilities and developing their methods of attack.*

## The challenge of keeping on top of things

In line with our earlier discussion, someone needs to be responsible for keeping track of evolving web security threats so you can ensure that appropriate steps are taken to protect your business against them.

*Someone needs to be responsible for keeping track of evolving web security threats so you can ensure that appropriate steps are taken to protect your business against them.*

This can be driven at a very detailed level internally, e.g. within your IT or security team. Intelligence reports produced by security vendors providing comprehensive information on the threats that exist out there, and how things are trending, can be exploited here. Figuring out what's relevant from industry data can be quite onerous to do thoroughly, however, which means that shortcuts are often taken. Most commonly the individual or team responsible will identify what they consider to be the most likely threats and focus on those. The trouble is you can then be caught out by something less obvious or a threat that has only recently emerged.

*Figuring out what's relevant from industry data can be quite onerous to do thoroughly.*

Even if you do a good job of keeping up with the threats, there is then the problem of coordinating protection. Responsibilities here can get very blurry, leading to key questions being left open, such as:

- What should software developers be doing to avoid security holes in applications?
- When a new threat emerges who should be responsible for making sure existing applications are not vulnerable?
- Do developers need to go back through the code and check it, for example, or should the operations team try to block the potential attack at a network level before it reaches the application?
- Who looks after 'security' if the web application is run on a service operated by a third party such as a hosted platform outside the business?
- Whose job is it to spot when an attack is taking place and establish if breaches have occurred?

Technical considerations are of course wrapped up in such questions, but a lot of the time it boils down to who is expected to take care of what, and issues such as the overhead and level of distraction involved often arise. With everyone focused on their core activities - developers on delivering new capability as quickly as possible, operations staff on maintaining service levels, etc - no one wants to spend time doing 'extra work' to take care of security matters.

*No one wants to spend time doing 'extra work' to take care of security matters.*

## Reducing both the burden and risk

One way of ensuring that the necessary teams and individuals take ownership and responsibility more willingly and effectively is to reduce the burden of what you're asking them to do. It's here that introducing the right kind of tools and services into the mix can pay dividends.

*Introducing the right kind of tools and services into the mix can pay dividends.*

As a simple example, today it is possible to sign up to a service with a supplier who keeps track of all web-related threats likely to impact your business. They then not only monitor your website on a continuous basis, alerting you when anything suspicious or dangerous happens, they also provide tools to help developers test their code and identify vulnerabilities. Some tools even recommend how to fix vulnerabilities when they're flagged up.

*Some tools even recommend how to fix vulnerabilities when they're flagged up.*

If your IT or security team comes to you with a funding request for tools and services, it's worth taking them seriously. The more you make life easier for those who need to be involved in web security, the greater the chances of them doing what's required. As importantly, your business ends up far less exposed.

*The more you make life easier for those who need to be involved in web security, the greater the chances of them doing what's required.*

## Focus on response

Tightening things up around web security in the way we have described, allows you to focus on how you will respond when an incident or breach actually occurs. With this in mind, it's worth reiterating the importance of coordinating activity across different groups within IT and the business, with appropriate escalation mechanisms defined as necessary. A combination of preventative measures and monitoring of early warning signals means fewer incidents will need to be managed. Your organisation will also be better able to respond quickly and effectively when an incident occurs, which in turn helps to minimise the level of damage or loss.

# The Bottom Line

Most cyber crime nowadays is driven by entities who are highly organised and disciplined. The techniques in use to penetrate your systems and steal your data or bring down your business are advanced and ever changing. Against this background, replying on technology magic bullets to protect yourself is a recipe for unwelcome surprises, commercial loss and reputational damage. You need to be as organised in your approaches to protection and response as the Black Hats are in their methods of attack, and this starts with a clear definition of ownership and responsibility. The framework outlined in this document is one way of defining what needs to be done.

*You need to be as organised in your approaches to protection and response as the Black Hats are in their methods of attack.*

# 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

Founded in 2001 and headquartered in Santa Clara, California, WhiteHat Security is the leader in application security, enabling businesses to protect critical data, ensure compliance, and manage risk. WhiteHat is different because we approach application security through the eyes of the attacker. Through a combination of technology, more than a decade of intelligence metrics, and the judgment of real people, WhiteHat Security provides complete web security at a scale and accuracy unmatched in the industry. WhiteHat Sentinel, the company's flagship product line, currently manages tens of thousands of websites – including sites in highly regulated industries, such as top e-commerce, financial services, and healthcare companies.

For more information on WhiteHat Security, please visit www.whitehatsec.com.

# Terms of Use