SecureWorks

Whitepaper

Contents

Securing the Enterprise in 2015

5 pragmatic steps to security

Executive Summary

As the security landscape has changed, so has the role of the Chief Information Security Officer. Previously a technical role, it has become more business focused. Now it reports to the board, using a business risk management perspective. Security has become a business enabler.

Accordingly, CISOs must take a proactive, pragmatic, business focused approach to security. This paper sets out five major areas of focus for the pragmatic CISO.

Executive Summary
(continued)

First, it is important to understand the extended enterprise and its associated risks. This means taking a data-centric approach, understanding that this data may be inside or outside the organization boundaries. It is imperative not to forget third parties, as they are often a major source of security risk.

Then take steps to identify and comprehend security issues by carrying out a high level maturity assessment, benchmarked against peers and best practices. It is essential to increase your visibility of these security issues with scanning and monitoring of events.

Next, build a culture of security across the organization. Ensure that everyone understands that no one is excluded from the responsibility of protecting data. There are no exceptions, not even for senior management.

Reinforce this by making sure everyone is thoroughly and regularly trained using a layered security awareness program.

Finally, recognize that the chances are that you will be compromised. Plan accordingly and be ready to respond.

All of these steps are much easier to do with an objective, strategic, security partner. As the role of the CISO has changed, so has the way the organization works with its security partners. Rather than engaging piecemeal technical services, today the pragmatic CISO maximizes effectiveness by forming strategic partnerships with expert security consultants.

Introduction

Security is now crucial in ensuring business growth, and subject to business risk calculations.

Tackle the threats today

There has never been a more urgent need for companies to focus on security. Cybercriminals are busier than ever, with targeted attacks against retailers, banks, and ongoing opportunistic phishing efforts. These compromises are increasing in number and sophistication. The first quarter of 2014 saw the second highest number of phishing attacks ever recorded.

At the same time, the role of the Chief Information Security Officer is evolving, with security stepping out of the technology wings and onto the business stage. No longer just a technical problem to tackle with new equipment, security is now crucial in ensuring business growth, and subject to business risk calculations.

These factors make it doubly important to understand how best to tackle security issues across the whole organization. This white paper describes a series of five pragmatic areas for an organization to focus on as part of their security strategy, with the spotlight on people and process. Concentrating on these areas will ensure that the organization is in the best possible position to tackle the security threats of today and those still to come.

The evolution of CISO

It makes sense to choose security consultants who combine a real depth of information security expertise with strategic management consultancy services.

Choosing the right consultants

The Chief Information Security Officer or CISO is the top security executive responsible for all aspects of information security. Over the years the nature of this role has changed.

Fifteen years ago, the CISO (or ‘Head of Security’ or ‘IT Security Manager’) was a technical role, with little management responsibility or leadership skill. The main focus of the role was fire-fighting and disaster recovery. By 2006 the role had become more business focused with the CISO acting as a conduit between the technical and management functions. Business skills were needed as the CISO aligned security strategy with business strategy.

By 2014, the role had changed entirely. No longer siloed from other functions, it is business risk focused with a holistic view of the enterprise and it may even report to the board. The emphasis broadens out from operational concerns towards wider issues such as privacy, data management, governance and compliance. Being able to approach the role from a business risk management perspective and to speak the language of business strategy is core to what the CISO does, as is board level support.

The relationship the CISO has with suppliers is changing too. Previously the information security business function reporting to the CISO might have maintained relationships with one set of specialist suppliers, while the IT security and security operations functions with another. That is increasingly no longer so. Now CISOs are looking to collaborative models with consultants, such as Dell SecureWorks, where a strategic partnership can support the integration of all the security services required.

To maximize the benefits of this relationship, it makes sense to choose security consultants who leverage in-depth information security expertise with strategic management consultancy services over management consulting generalists with a single security offer. Choosing the former, sets an organization up for success by matching the changing needs of the CISO with a broader, deeper service offering. This is more effective than solely relying on technical assistance or management consultancy. It allows for a more strategic partnership.

Five pragmatic steps to security

A truly secure enterprise will always be compliant. In contrast, a compliant enterprise may not be truly secure.

Developing a security strategy

As the role of the CISO has evolved, so has the best approach to security. Now the focus is on proactively identifying business priorities, risk and engaging with the board. Benchmarking and metrics become critical as the board leaders wants to match or exceed industry norms to avoid becoming an easy target.

Previously security was all about saying, "No". Now the new focus on business requirements means that the security function is a business enabler. Enterprises are finding ways to embrace technologies safely that were previously deemed too dangerous, such as cloud and BYOD.

The perfect strategic partner will help the CISO develop a security strategy that is risk based and pragmatic, focused on priorities and low hanging fruit to maximize returns.

This strategy will:

- be people and process driven rather than focused on quick technology fixes,
- recognize that the company *will be* compromised at some point,
- prioritize the ability to respond quickly and appropriately.

The partner will show the CISO that this strategy must go beyond basic compliance. A truly secure enterprise will always be compliant. In contrast, a compliant enterprise may not be truly secure.

There are five pragmatic steps to achieving this aim.

Step 1

1. Understand the extended enterprise

The first thing any security strategy needs is a clear understanding of scope. What needs to be protected? It's no longer enough to assume that anything outside the perimeter is insecure and anything inside is secure. Today, de-perimeterisation resulting from cloud, home based working and mobile devices means that a broader, data-centric approach is more appropriate. Recognizing that the data and its users may be inside or outside the organization is key.

To gain this understanding, map out the business and security's place in it. Look both within and outside the organization's boundaries and learn the processes of the business. Also, familiarize yourself with its different teams by understanding their roles and goals over the short, medium and long-term. Only by knowing what is important to the business can you define security's role within it.

Step 1
(continued)

Understand the extended enterprise

This process must include identifying third parties, for they are a genuine part of the extended enterprise. Ensure security is applied in agreements with them and make certain that those third parties are regularly assessed.

Failure to understand and mitigate the risks of the extended enterprise was likely to have been a key contributing factor to a large retailers breach in 2013. The compromise was widely attributed to its refrigeration contractor that fell victim to a phishing attack. It is believed that a compromised credential allowed the attackers to gain access to the retailers network, stage further attacks to gain access to the POS network, place card-stealing malware on every POS system, steal millions of cards and cause hundreds of millions of dollars in damage. The overall cost to the financial sector in replacing cards compromised by the attack has topped $200 million. By mapping out who has access to your systems, auditing those suppliers to ensure best practices are being carried out, ensuring critical systems are appropriately segregated from non-critical users and enforcing two factor authentication for all third-parties, incidents like this can be avoided.

Next, build a register of your critical information assets and classify them. These could include intellectual property, card data, personal data, information about mergers and acquisitions and more. Know where they are, how they're protected and who has access to them and whether those with access rights are inside or outside the business perimeter.

Finally, identify risks to key information assets and prioritize those risks according to business needs. A risk based approach is essential to achieving compliance with standards such as ISO 27001.

Often this whole process can be hard to do internally, maintaining objectivity while benchmarking against current industry best practice. This is why a strategic partnership with a security consultant can provide a clear picture of assets that a purely internal team may overlook. Dell SecureWorks has a defined methodology to help customers map out their business and risks. While this can form the foundation of an ISO27001 certification, it's often used by customers who simply want to build a clearer picture of their organization.

Step 2

2. Increase visibility into what's going on in your environment

Next you need to understand where the security issues lie. Dell SecureWorks calls this 'increasing the aperture of visibility'. This requires making sure you have as much information as possible and, just as important, looking at available information in the right way to prioritize investment and response efforts.

This should involve high level business and low level technical activities. A high-level security maturity assessment against industry best practice, standards and peer groups can help management understand strengths, weaknesses, gaps and areas for improvement. Furthermore, it is a crucial input into any organization's security strategy.

At the technical level, on a frequent and ongoing basis, increase the visibility of activities such as:

- collecting and monitoring security events from all your security infrastructure,
- deploying intrusion detection systems to monitor network and endpoint activity,
- scanning infrastructure and applications for vulnerabilities and
- penetration testing.

All of this should be backed up by applied threat intelligence and robust processes for patch and configuration management.

Step 3

3. Build a culture of security

Good security comes from people and process rather than technical fixes. But, transforming attitudes to security within the enterprise is one of the hardest jobs the CISO will face. For far too many people believe security is purely the job of the CISO and has nothing to do with them. All people in an organization need to understand the risks they face and how important their specific role is in taking ownership for secure practices.

To embed security into the whole organization, everyone must be responsible for their own role in protecting information. There must also be someone in each department who is accountable for security. These stakeholders from across the organization should then form a steering group that ensures that important information regarding security is filtered down to all parts of the organization.

Last but not least, top management must commit to security. This isn't just to enforce it on lower management. All too often, senior management feel they can flout security rules. However, the people in leadership are typically the top target for attackers. To build a true culture of security, there can be no carte blanche exceptions.

Step 4

4. Train your users

The number one risk most organizations face today is from reckless actions by employees who don't understand security, the risks, or the impact of their actions. In some cases, they simply don't care. That makes training them absolutely crucial.

Most targeted attacks today exploit end users through spear phishing and social engineering. Making sure your staff members know that they are targets and understand how they should respond is one of the most important ways of securing company assets.

While training certainly forms a vital part of embedding a culture of security, it requires extra focus. Many organizations believe standard training modules from compliance programs are enough to ensure education on security.

They are not.

Instead, addressing the weakest link and building a layered security awareness program with security essentials, organization-specific training, and role-specific exercises is a more effective training strategy.

This includes training up, as well as down – it's not enough for senior management to be aware of security. Instead of seeing it as a constraint, they must see that it is crucial to business growth.

Remember that training isn't a one-off exercise. Every three months is optimal. Annually should be the bare minimum. Testing regularly, with security surveys and phishing tests are advised, If necessary, you should offer targeted remediation training.

Step 5

5. Be prepared to respond to incidents

However good your awareness, however effective your training, the chances are that one day, you may be compromised. This is just one reason why improving visibility of security is so important within the enterprise.

It pays to operate under the assumption that you are already under attack and are ready to respond. Being agile and responsive in the wake of an IT security breach will help you minimize the damage.

Remarkably, incident response remains low on the agenda for many organizations and is still one of the most overlooked areas in information security. With cyber-attacks on the increase, organizations need to prioritize their incident response plan and build a proactive, ongoing incident management program to counter any future security breach. If you accept the premise that you are already compromised, doesn't it make sense to focus on limiting damage and disruption to business operations?

There are several steps to this preparation:

- First build tried and tested incident response processes, with clearly defined and formalized roles and responsibilities.
- Understand where your logs are and how to get access to them in the midst of an incident. This includes across organizational boundaries and from cloud service and other external providers.
- Don't assume that your contract with cloud and other providers automatically allows this. Mid-incident is no time to start contract renegotiations.

Similarly, pre-arrange vital relationships with security suppliers and service providers so that you can call on them immediately. A true strategic partnership with a consultant will make a critical situation much easier.

And in a climate where the majority of organizations are a genuine target of cyber-attack, it's worth regularly evaluating your incident response plan to ensure you are prepared. Remember, it's not *if,* but more likely *when* you are at the center of a security incident.

Conclusion

Know what assets you've got, where they sit and whether they are vulnerable to exposure.

If you do nothing else, do this

Dealing with each of these five areas will place your organization in a much better position to deal with the inevitability of compromise in the modern business environment.

However, if there's one thing that Dell SecureWorks understands, it's the importance of pragmatism. So, if you were going to do just one thing after reading this paper, what should it be? Most importantly, it should not be simply throwing money at the latest security technology. Bluntly put, technology isn't the core answer to pragmatic security and it can even be the enemy. Far more important is knowledge and awareness. Technology can be an enabler, but it's not the final destination.

Instead, if you do just one thing, make sure it involves knowing what assets you've got, where they sit and whether they are vulnerable to exposure. Ask yourself, where is your data? What infrastructure does it sit on? Which of your data assets are Internet-exposed? If applicable, where is your regulated data? And just how necessary is the data you are storing?

That in itself will stand you in excellent stead. Finding a strategic partnership with a trusted security expert that can assist you in all the aspects of information security is vital. Dell SecureWorks is a market leader in security that can close the security gap in organizations by evaluating security maturity across an enterprise, help define security strategies, and implement and manage security program plans. We are a true strategic partner that can help a CISO embed security at all levels of the organization.

About Dell SecureWorks

A trusted global partner

Dell SecureWorks is relentlessly driven to protect the integrity of the world's digital assets against cyberthreats. We do that with intelligent defenses that combine our proprietary technology, global threat visibility and deep expertise. We are 100% focused on information security – it's all we do. That's why we are trusted by thousands of customers. Dell SecureWorks offers a full suite of Managed Security, Threat Intelligence and Security and Risk Consulting services.

SecureWorks

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

January 2015.