GlobalData.

The Role of Human Resources in Managing Cybersecurity

D. Kehoe

October, 2016

GlobalData.

The Role of Human Resources in Managing Cybersecurity

Summary

Issue

The IT security industry is undergoing a transformation. The number and type of security attacks continue to proliferate at a time when the underlying infrastructure is moving from a physical environment to one that is virtualised and mobile enabled. GlobalData research shows that 67% of HR directors in Australia play a role in delivering IT tools and access policies based on employee roles. While HR is not the sole guarantor of cyber security, this department is playing a central role in ensuring access policies are implemented correctly and that end users are given some level of education and training. When breaches do occur and there are cases of company embarrassment, loss of intellectual property, financial losses or executive resignations (or worse), HR plays some role in establishing policies and business processes in response to a data breach. For major events, there will often be an HR handbook for internal communications and escalation procedures.

Key Takeways

People are the greatest asset to an organisation, but can also be the greatest threat and single largest point of vulnerability when it comes to information security.

Security breaches are happening daily and up to 80% of Australian businesses believe they may have been victims of data breaches.

Most organisations have no formal programmes in place to promote security awareness or train employees on their own IT policies.

Assume a security breach will happen, but what will set HR apart is having a plan beforehand that it can act on when one occurs.

Technology can be effective in the recruitment and retention of staff. It is important that security and end-user experience balance out and employees have the best tools for the trade.

Perspective

Current Perspective

People are the greatest assets in an organisation. In a survey of 200 Australian HR directors, the top corporate priority for the next 12 months for HR is to build up leadership at all levels, increase employee engagement and reduce turnover. However, when it comes to corporate information security, employees are often the weakest link. The vast majority of Australian businesses believe that they may have fallen victim to data leakage. This is a mixture of accidental leakage (80%), having employees targeted by outsiders (nearly 60%), and/or the malicious insider (50%) leaking or stealing corporate data. Many organisations in the survey cannot determine if any breach has even taken place, or what information may have been found. While it takes second or minutes for a breach to take place, industry research shows that it will take weeks or months for an event to get noticed – if at all.

While there are many threat vectors for a data breach, some of the largest and most damaging attacks have come from the insider. In general, there are three types of insider data breaches: careless insider (e.g., the employee that accidently leaks corporate data); the targeted insider (e.g., the employee that is targeted through social engineering, phishing or other means); and the malicious insider (e.g., the employee that steals or intentionally leaks corporate data). While HR plays a number of different roles in these domains, education and training can go a long way in preventing data leakage from the insider. HR should also have pre-defined policies in place and escalation procedures during and after a cyberattack. This should be in partnership with other lines of business leaders, CXOs, boards and others, including external parties that need to be involved. This report considers five steps HR directors should consider for managing cybersecurity through their own department initiatives.

1. Increase Companywide Training and Awareness

Studies show that while the insider threat can do the most damage, the vast majority of instances are around the careless and targeted insider. One of the most prolific data breaches caused through social engineering occurred at Anthem, the U.S. health insurance provider. This single event topped Forbes Magazine's 'Top 10 Security Breaches of 2015.' While an investigation is ongoing, internal employee credentials were attained by outsiders and up to 80 million health records were lost. This is equivalent to 1.4 million sheets of A4 paper. The Ponemon Institute estimates the average global cost of data breach per lost or stolen record was $355 for a healthcare organisation.

HR can play a major role in education, training and general awareness to protect employees from being targeted and educating them on security policies. HR can also play a role brokering conversations between the end users and IT departments so that there is an ongoing 'feedback loop' and policies are not rolled out in isolation or in environments where end-user needs and experiences are ignored. Fostering collaboration is a top requirement for HR managers and this is one way to deliver an outcome to protect corporate data and intellectual property. One CISO acknowledged to us that 'end users have a right to complain and need a feedback button so IT can improve.' A number of organisations have also conducted the 'fake phishing attack' as a way to measure security awareness within the company. Continuous education can also help to start changing those bad habits (e.g., password sharing, writing down credentials on Post-it notes to stick above the screen) and mitigate the threats caused by the careless users.

2. Build Up the Security Competencies

Security is a global challenge and the lack of skills is real. There are up to one million security jobs that go unfilled globally each year. From this figure, GlobalData estimates that as many as 50,000 security jobs go unfilled in Australia. To compensate for this talent shortage, HR strategies should consider partnering with universities as a means of recruiting and training new sources of talent. Security competencies should be embedded in the next talent pool. Security should not focus solely on a finite area, but take inputs from all aspects of security, including technology and compliance as well as financial, socio-economic and legal factors. While a number of companies have colocated facilities on or near a major college campus to find flexible working for contact centre staff to better serve customers, for example, few companies have even looked at ways to use talent pools in academia for cybersecurity. Industries that are heavily regulated such as government, financial services and education must consider additional measures to increase the security awareness and competencies within their organisation.

3. Assume a Breach Will Happen on Your Watch

It is a best practice for companies is to assume that not all breaches can be prevented and one will happen on your watch. From an HR perspective, having the right policies and escalation procedures in place is important to contain the threat and to control the overall damage that it may have on employees, customers and/or the company brand. This could be in partnership with corporate communications, legal and financial teams. Data breaches which are caused by malicious insiders may require formal polices for how to notify senior management, legal counsel and potentially law enforcement. The important consideration for HR is having a plan in place when a data breach does occur. The 2013 Target breach is a great case study for the industry on how not to respond. It was a case of endless internal discussion, board meetings and failure to act until it was too late.

4. Work with the IT Department

IT departments are generally aware of the various threats and will focus on reducing the time between the discovery of a breach and resolution. The closer these metrics are, the less damage a security breach will likely cause in an organisation. However, it is often the case that organisations do not know what they actually own, cannot assign a value to the data or struggle to find an 'owner.' It is advisable for lines of business, such as HR, to go through this exercise in at least creating a data classification system. From this point, it becomes easier to consider technologies such as data loss prevention, which tags, maps and fingerprints data in a classification system. It is used by companies to prevent data from leaving a private network to an unauthorized destination, such as the public Internet, personal e-mail addresses or USB storage. DLP can often be used in combination with analytics engines to provide 'context' IT activity. The solution typically works by creating a baseline of 'normal' activity and setting up a platform that can provide alerts when anomalies are detected. A large Australian insurance organisation was able to detect fraud within the first days of implementing such a system and had a system set up to notify HR, hiring managers and law enforcement. In the end, the plan was foiled, the company saved millions, the matter was turned over to the police and the solution paid for itself.

5. Balance Security Requirements with the End-User Experience

Despite the security threats, employees need to access cloud services, share collaboration tools and use mobile devices inside and outside the office. Many organisations have also moved to a BYOD culture. The recent GlobalData survey found that 65% of HR directors saw the need to provide the same HR policies for employees inside and outside the office as 'important or very important.' As new employees are on boarded, and others promoted or move between departments, HR can work on policies that support access privileges which are role based. With new tools, these privileges can be automated and policy enforced. HR can protect corporate data assets by working with IT and identifying those policies. Many businesses are also offering flexible working and IT tools to attract new talent. Security in remote access, mobile devices, applications and corporate networking will continue to be paramount, as will the need for ensuring end users can enjoy a high user experience. This will also reflect on customers and important considerations for digital transformation.

Recommended Actions

Buyer Actions

Most organisations lack the basic security discovery capabilities. As part of this exercise, IT and lines of business need to ask basic questions, such as the location of their corporate data, and consider assigning values around classes of data. HR's role would be to help determine who in the organisation should have access to what data. IT can look to apply security measures proportional to the value of the data.

The cause of a data breach varies, but most organisations in Australia interviewed by GlobalData have found it difficult to find funding for basic security awareness. Simple steps such as setting up a formal training programme to encourage employees to follow IT procedures for sending a file or managing corporate data can go a long way. These initiatives are typically funded by HR as part of employee education and training.

Basingstoke

4th Floor, Northern Cross
Basing View, Basingstoke,
Hampshire, RG21 4EB,
UK
+44 (0) 1256 394224

Beijing

Room 2301 Building 4
Wanda Plaza, No 93 Jianguo Road
Chaoyang District
Bejing 100026, PR China
+86 10 6581 1794
+86 10 5820 4077

Boston

179 South St, Suite 200,
Boston, MA 02111
USA
+1 617 747 4100

Buenos Aires

Basavibaso 1328, 2nd Floor
Off 206, Buenos Aires, 1006
Argentina
+54 11 4311 5874

Dubai

Dubai Media City
Building 7, Floor 3, Office 308
PO Box 502635
Dubai
United Arab Emirates
+971 (0) 4391 3049

Hong Kong

1008 Shalin Galleria
18-24 Shan Mei Street
Fo Tan, New Territories
Hong Kong S.A.R
+852 2690 5200
+852 2690 5230

Hull

GlobalData PLC
Shirethorn House
37-43 Prospect Street
Hull
HU2 8PX

Hyderabad

2nd Floor, NSL Centrum,
Plot No-S1, Phase 1 & 2
KPHB Colony, Near: BSNL Office
Hyderabad-500072
Andhra Pradesh
+91-40-30706700

London

John Carpenter House
7 Carmelite Street
London
EC4Y 0BS
+44 (0) 207 936 6400

Madrid

C/Jesusa Lara, 29 – Atico J,
28250 Torrelodones Madrid,
Spain
+34 91 859 4886

Melbourne

Suite 1608
Exchange Tower
Business Centre
530 Little Collins Street
Melbourne
3000, Victoria, Australia
+61 (0)3 9909 7757
+61 (0)3 9909 7759

New York

441 Lexington Avenue,
New York, NY 10017
USA
+1 646 395 5460

San Francisco

Progressive Digital Media Inc
425 California Street
Suite 1300
San Francisco
CA
94104
USA
+1 415 800 0336

Seoul

Global Intelligence & Media Korea Limited
11th Floor, West Wing,
POSCO Center Building,
892, Daechi-4Dong,
Gangnam-Gu, Seoul 135-777
Republic Of Korea (South)
+82 2 559 0635
+82 2 559 0637

Shanghai

Room 408, Jing'an China
Tower No: 1701,
West Bejing Road
Jing'an District, 200040,
Shanghai, PR China
+86 (0)21 5157 2275(6)

Singapore

1 Finlayson Green
#09-10
049246
Singapore
+65 6383 4688
+65 6383 5433USA
+1 415 800 0336

Sydney

Level 2
63 York Street
Sydney
NSW 2000
Australia
+61 (0)2 8076 8800

Tokyo

Global Intelligence & Media Japan Tokoyo
Level 3,
Sanno Park Tower,
2-11-1 Nagata-cho,Chiyoda-ku,
Tokyo, 100-6162
Japan
+81 3 6205 3511
+81-3-6205-3521

Toronto

229 Yonge Street
Suite 400
Toronto
Ontario
M55B 1N9
Canada

Washington

21335 Signal Hill Plaza,
Suite 200, Sterling,
VA, 20164
+1 703 404 9200
877 787 8947 (Toll Free)