The Economist INTELLIGENCE UNIT

Cyber insecurity: Managing threats from within

Briefing paper

Sponsored by:

proofpoint.

Contents

3 About this report

4 Introduction

5 Confronting data breaches

6 The people factor

7 Addressing data breaches

11 Obstacles to best practice

13 Conclusion: The way forward

About this report

Cyber insecurity: Managing threats from within is an Economist Intelligence Unit report, sponsored by Proofpoint. To explore the frequency and severity of people-centric data breaches, the EIU surveyed more than 300 corporate executives, including CIOs, CISOs and other IT executives, finance and line-of-business leaders, with roughly equal numbers located in North America, Europe and Asia/Pacific.

The EIU supplemented the survey results with in-depth interviews with senior executives. We would like to thank all survey respondents for their time and insights. Eric Laursen wrote the report and Gilda Stahl was the editor.

The following senior executives (listed alphabetically by company) were interviewed for the research programme:

- Adrian Ludwig, CISO, Atlassian
- Deborah Wheeler, CISO, Delta Air Lines
- Prasanna Ramakrishnan, global head of information security risk, Signify (previously Philips Lighting)

Introduction

Data breaches, defined broadly as the intentional or unintentional release of secure or private/confidential information into an untrusted environment, are a rapidly growing problem for businesses worldwide. People-centric threats—from phishing to lost or stolen devices to activity on an unsecure network to lost or stolen passwords—can be at least as crippling as more arcane technical glitches and oversights.

This poses a delicate problem. While companies can exert some control by introducing better security measures such as two-factor authentication, centralised logging, and restrictions on web browsing and personal email, they must ultimately depend on human beings to follow best practices and share information about incidents, which can help them anticipate and prevent similar events.

To gauge the frequency and severity of such weaknesses, their causes and the steps companies are taking to address them, The Economist Intelligence Unit surveyed more than 300 corporate executives, including CIOs, CISOs and other IT executives, finance and line-of-business leaders, with roughly equal portions located in North America, Europe and Asia/Pacific.

Confronting data breaches

Data breaches are having increasingly disastrous consequences for business. As a result of a massive 2017 data breach that exposed the personal identity information of more than 148m people, Equifax in July agreed to pay US$425m to help the victims and US$275m in civil penalties—the largest such monetary settlement to date.

An overwhelming majority (86%) of survey respondents say their organisation has experienced at least one data breach in the past three years, with well over half (60%) saying they have experienced at least four. Large companies (US$500m or more in annual global revenues) are especially vulnerable; more than two-thirds (68%) have experienced at least four data breaches in the past three years, compared with 53% of smaller companies.

Data breaches disrupt businesses in a variety of ways. Survey respondents most frequently cited the following in their top three: loss of revenue (33%), especially at large companies (38%); loss of clients (30%); and termination of staff involved (30%).

The problem is only growing.

Nearly half of survey respondents (47%) say it's very or extremely likely that they will face a major data breach in the next three years. Not surprisingly, companies that have experienced one or more data breaches in the past three years are far more likely to anticipate another one in the next three years than companies that haven't (53% vs. 9%[1]).

Many companies, however, are still in the early stages of devising an effective strategy for preventing and responding to data breaches—mitigating their effects. "Not everybody understands yet that a huge company can be brought to its knees by one of these attacks," says Prasanna Ramakrishnan, global head of information security risk at Signify (formerly Philips Lighting). "We have to be able to get to a predictable structure of security."

> **"Not everybody understands yet that a huge company can be brought to its knees by one of these attacks.**
>
> *Prasanna Ramakrishnan, global head of information security risk, Signify*

Impacts of data breaches

(% of respondents)

[1] This figure was taken from a small base, but trend is directional.

The people factor

While companies in all industries are growing ever-more technology-driven, their exposure to people-centred threats also continues to worsen. Even at an industrial company like Signify, these internal threats are among the most serious, says Mr Ramakrishnan. "Intellectual property is our most important asset," he says. "As a global company, we have a significant presence all over the world, and so we must constantly balance managing the potential threats with running our business without interruption."

Most cyber-security breaches are the result of human vulnerabilities, not a failure in technology or process. Most serious are people-centric threats, phishing, ransomware and other malware, business email compromise and wire transfer fraud, which nearly half (48%) of respondents cited as collectively a top-three risk.

While system misconfigurations and accidental exposures are the second most frequently cited vulnerability, others that our respondents mention are all driven by human error:

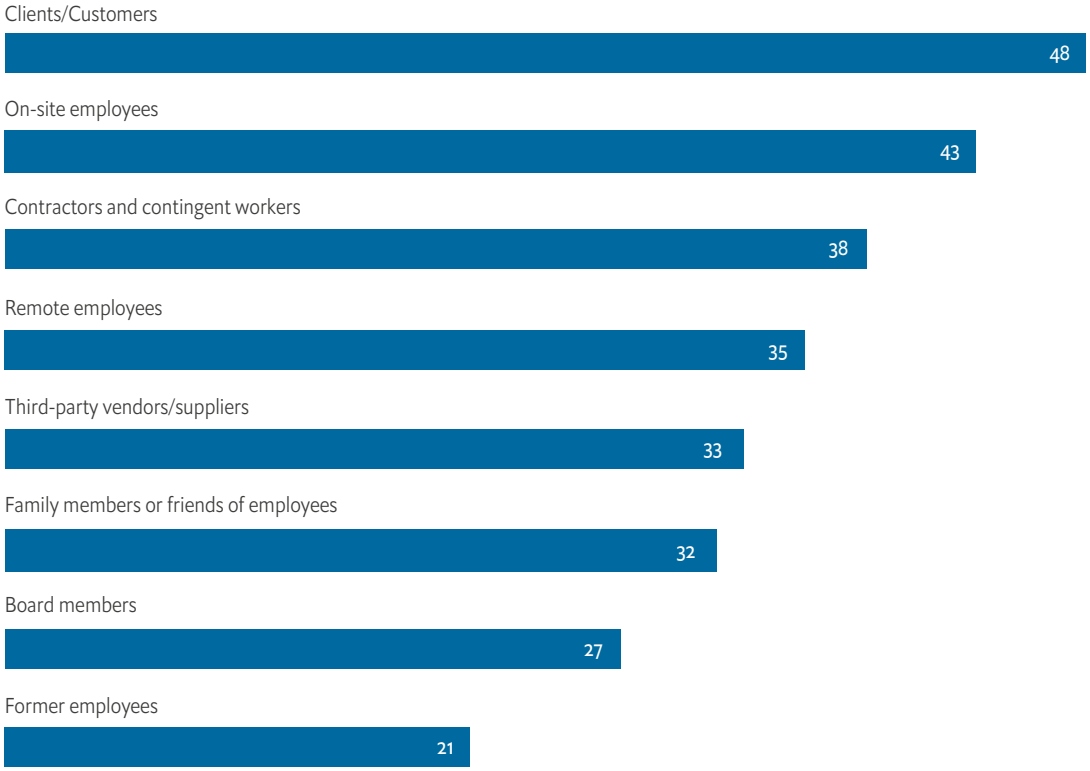
- Lost, stolen or otherwise hacked devices (33%);
- Unpatched software vulnerabilities (32%);
- Activity on an unsecure network or location, such as airport or coffee shop (31%); and
- Lost or stolen user names and/or passwords (29%).

Where do attackers look to exploit vulnerabilities? Clients and customers are the group most often targeted in data breaches (48%); the next most likely are all either employees, contractors or people closely connected to them.

This finding underscores the reality that network vulnerabilities can easily extend beyond the company's area of direct control. It also highlights the need for companies to understand the degree to which some employees, because of their visibility, work routine or level of data privilege, may be more vulnerable to attacks than others.

A high-profile employee may be the target of more sophisticated malware attacks; one who has access to the CEO may be hit by phishing attacks that spoof the CEO or other executives. Assessing vulnerability involves considering such factors as what cloud apps the employee uses, how many and what devices, their level of access, how frequently they are targeted and, of course, whether they practise good digital hygiene.

Targets of data breaches
(% of respondents)



Addressing data breaches

Reducing the risk of a major data breach has become a top area of concern at most companies. An overwhelming 82% of survey respondents cite it as a high or essential C-suite priority and 73% expect reducing the risk of a major breach to become a higher priority for the C-suite over the next three years. Almost all respondents (96%) say the board and C-suite strongly support efforts to control cyber-security risks and 93% say the board and C-suite are regularly updated on cyber-security risks.

Adrian Ludwig, CISO of Atlassian, an Australian enterprise software company, issues monthly cyber-security reports to the executive team and quarterly reports to the board. "We let them know if there's a gap, and if we need more investment, it's an easy conversation," he says.

How are companies addressing data breaches? For many, it starts with centralising the organisation's efforts to help create a cyber-security culture embracing every employee, every functional area and line of

business and the networks that bind them together. Virtually every respondent (94%) agreed that their organisation has done so.

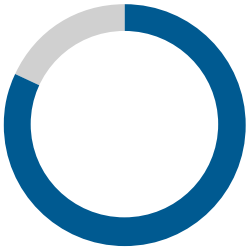
A related measure is moving corporate infrastructure to the cloud to ensure a more secure data environment. Almost half (46%) of respondents say their organisation has moved more than half of its data infrastructure to the cloud and over 69% say they have moved more than 40%. Most respondents also say their organisation has undertaken processes to address data breaches. The survey divided these into two groups: processes to ensure responsible cyber-security behaviour by employees and processes to avoid and mitigate data breaches.

Between 84% and 95% of respondents say their organisation has taken action or plans to implement the following to ensure responsible behaviour:

- Conduct pre-employment screening and background checks to avoid hiring individuals who pose a risk (89%);
- Require employees to sign confidentiality agreements (91%);
- Develop and enforce information security policies for employees (93%);
- Conduct regular employee education and security training (94%);
- Limit or block personal web browsing and access to personal email (91%);
- Define and limit employee access to specific data types (95%);
- Offer incentives to motivate upstanding online behaviour (84%);
- Stipulate clear consequences for negligence (91%); and
- Monitor user accounts for unusual activity or behaviour (94%).

Between 86% and 96% say their organisation has taken action or plans to implement the following to avoid and mitigate data breaches:

- Require strong credentials and multi-factor authentication (93%);
- Train users to detect and report suspicious email (94%);
- Isolate employees' personal web browsing and email activity from network traffic (92%);
- Implement a zero-trust network strategy for access security (86%);
- Install security programs (secure email gateways, cloud access security broker/ cloud security tools, firewalls, anti-malware and anti-virus software; 96%);
- Roll out systems and software updates and patches as soon as they are available (94%);
- Install upgrades as soon as manufacturer no longer supports software (95%);
- Periodically run tests on data security standards and practices (96%); and
- Require use of a virtual private network (VPN; 91%).



82%

cite reducing the risk of a major security breach as a high or essential C-suite priority; 73% expect it to be a higher priority over the next three years.

At Delta, "we take a risk-based approach" to cyber-security, embracing not just company-specific data but employees' and contractors' own PII [personally identifiable information] and PCI [payment card industry] data, says Deborah Wheeler, CISO at Delta Air Lines. "So a lot is based on the data itself."

Delta has already taken most of the actions listed above, resulting in a defense-in-depth structure that includes security portals when the user enters the Delta network, additional challenges for each specific system, and then monitoring of and controls over how the data can be treated by the end user.

"At every step of the user's data experience, some form of control is happening," she says. "Our team is never done; we are constantly reviewing and altering our approach to account for the ever-changing threats and approaches by bad actors."

Like other large companies, Delta has also started testing adaptive security architecture to "track user behaviour, view what's happening in the environment and make adjustments", Ms Wheeler says. It's a still-developing area, she adds, and "there's still a good deal of human interaction to ensure that appropriate actions are taken when suspicious activities are detected".

At times, the technology "attempts to remediate where there was not an actual covert action". As adaptive security matures, however, "it will free up our analysts to tackle bigger problems in our environment".

What works best?

Respondents' views on the effectiveness of security processes vary considerably. The most favoured tend to be the most basic, suggesting that as long as employees are educated and informed of the rules, they will assume a measure of responsibility.

Survey respondents who had already implemented security processes found the following to be most effective in ensuring responsible cyber-security employee behaviour: conducting regular employee education and security training (35%) and developing and enforcing information security policies for employees (34%). In addition, one out of four respondents mentioned limiting or blocking personal web browsing and access to personal email.

Most effective security processes* for ensuring responsible employee cyber-security behaviour
(% of respondents)

* Survey question addressed to respondents who had already implemented security processes.

To work well, cyber-security education and training must actively engage with employees, says Mr Ludwig. "A lot of it is raising awareness and building tools so that they will have visibility into their situation," he says. That means monthly check-ins with each production area, including employee behaviour such as whether they are using correct authentication when signing on.

Keeping in mind that at Atlassian, most employees are technologically sophisticated, "I focus on making sure the easy way to get things done is the most secure way," Mr Ludwig says. "When I find corner cases where someone is doing it differently, I show them that if they make these tweaks, it will be more secure."

Bringing employees as close as possible to the actual experience of a breach is key to making cyber-security training effective. At Delta, which has never had a breach[2], "we try to act as though we've just had a breach," says Ms Wheeler. The company runs red- and blue-team simulations as part of its programme. At Signify, "We emphasise continuous learning. For example, when an employee shares with us that they have experienced unusual activity via social media, we will use that story as an example throughout the organisation to raise awareness and create a teaching moment," says Mr Ramakrishnan.

However, education and security training alone will never be 100% effective, he adds: "We recently implemented a security test for our employees. Twenty percent followed through immediately; 50% were in the middle, wondered why we were doing it and needed subject matter experts to explain it to them; and 20-25% will never do anything." With that last group, "we go through a multi-step process to raise awareness, compliance and alignment to improve that number."

By contrast, the processes least favoured by survey respondents to improve employee behaviour are more impersonal: pre-employment screening and background checks to avoid hiring individuals who pose a risk (21%) and offering incentives to motivate upstanding online behaviour (16%).

The processes considered most effective by far in avoiding and mitigating data breaches are installing security programs such as secure email gateways, cloud access security broker/cloud security tools, firewalls, anti-malware and anti-virus software.

At Atlassian, "we have two-factor authentication," Mr Ludwig says, "and we're working with our vendors to make sure they're all up to speed. We want centralised authentication for all of them."

The company also enforces tiered access services within its corporate environment. It takes a comprehensive, centralised approach to logging corporate activity, balanced with processes designed to protect employee privacy.

The two most important specific processes, Mr Ludwig says, are single sign-in across all applications and centralised logging, "so that if there's an incident, we can investigate quickly".

Other choices depend more on individuals' training and behaviour: requiring strong credentials and multi-factor authentication (29%), training users to detect and report suspicious email (also 29%) and isolating employees' personal web browsing and email activity from network traffic (23%).

"We look at access logs," says Mr Ludwig. "So, for example, if there's a portal that provides access for support personnel to help customers with problems, in what scenario is it being used and with which controls?"

> **"I focus on making sure the easy way to get things done is the most secure way. When I find corner cases where someone is doing it differently, I show them that if they make these tweaks, it will be more secure.**
>
> *Adrian Ludwig, CISO, Atlassian*

[2] [24]7.ai, a service that provides online customer chat for its clients' websites—which included Delta—experienced a data breach in 2017.

Obstacles to best practice

Respondents largely express confidence (76%) in their organisation's ability to prevent, detect or respond to data breaches. But some are less sure than others—at healthcare companies, a bare majority agreed (56%). And our survey reveals significant weaknesses in companies' efforts to minimise people-centric risks.

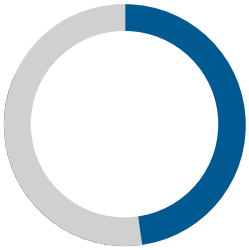
Perhaps the most serious of these is ensuring effective cyber-security behaviour by employees with contractors, contingent workers and other vendors. "This is absolutely critical," says Ms Wheeler. "A large company like Delta works with a lot of third parties, and, as a result, they have opportunities to come into contact with our systems. We have the same expectations for them as for our employees, based on contractual obligations around our assets, and we review high-risk vendors on an annual basis."

Especially as manufacturers adopt the Internet of Things (IoT), this issue will become more urgent. "We work with a number of third-party vendors and collaborate across the industry to develop products," says Mr Ramakrishnan. "Companies can be at different stages in their security journey, which can bring inherent risk that we have to manage."

Yet less than half of respondents (48%) say pre-employment screening and background checks are applied equally to contractors and contingent workers. A substantial group (37%) says they apply only to full-time employees. Similar numbers apply to confidentiality agreements, development and enforcement of security policies, regular education and security training, and limiting and blocking personal web browsing.

A lack of dedicated leadership appears to be a widespread problem: EIU research suggests that many—if not most—companies still do not have a dedicated individual in charge of cyber-security.

Only 24% of respondents named a CISO or head of IT security or equivalent as being most directly responsible for addressing cyber-security at their organisation, while 26% named the CTO and 15% cited the CIO or head of IT. Other respondents spread the responsibility among a variety of positions, including CEO/owner/partner or equivalent (12%).



48%

Less than half of respondents say pre-employment screening and background checks are applied equally to contractors and contingent workers.

Co-operation isn't the issue

Indeed, the biggest obstacles to implementing and enforcing best practices for reducing the risk of employee-related data breaches appear to be management and control-related, rather than lack of co-operation by employees, vendors, contractors or other outside parties.

"Vendors are the number-one area where we face the biggest obstacles, and always the most time-consuming," says Ms Wheeler. "Many don't appreciate the risk in the applications they're providing, but it's our job to ensure that their tools meet our high standards before they're implemented."

Poor or inconsistent enforcement of data access policies was most commonly mentioned as a leading problem by survey respondents, followed by difficulty co-ordinating policies across LOBs and functional areas (24%) and lack of funding or support for employee education and security training (24%).

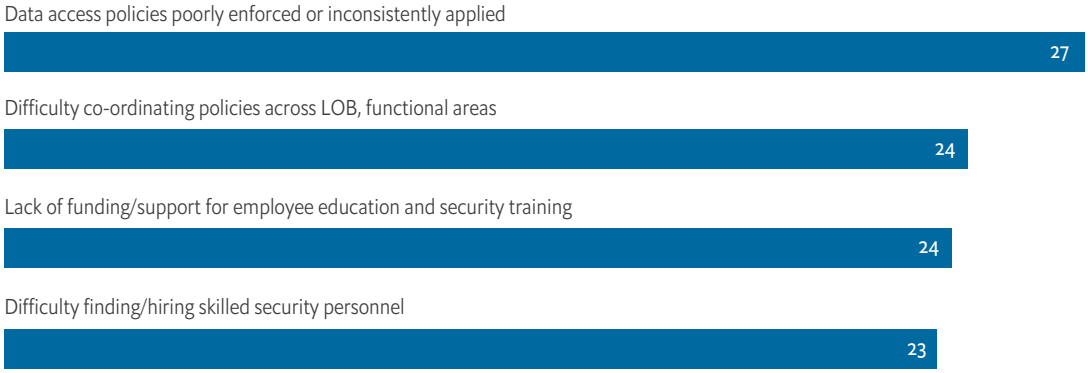
"Unfortunately, every security leader I've spoken with agrees that data security has a long history of poorly defined expectations and poorly implemented technology that one way or another makes security difficult," says Mr Ludwig.

Much further down the list are low levels of co-operation from employees (21%), independent contractors/contingent workers (also 21%), clients/customers (15%), vendors/suppliers (14%), and lack of C-suite support (15%).

The solution to many employee-related cyber-security problems, then, may be better enforcement and co-ordination of existing policies and better funding of cyber-security efforts in general. But levels of co-operation among employees and other network participants appear to be generally good.

> **Vendors are the number-one area where we face the biggest obstacles, and always the most time-consuming.**
>
> *Deborah Wheeler, CISO, Delta Air Lines*

Obstacles to best practice
(% of respondents)



Conclusion: The way forward

The biggest obstacles to overcoming people-centred cyber-security threats are, of course, people themselves. "People have a lot to do, and while they care about security, they don't think about it amidst revenue targets and other goals," says Mr Ludwig.

What can organisations do to strengthen the people element in cyber-security? Looking into the future, most survey respondents already have part of their course plotted out. Survey respondents agree that the IT function must focus more strongly on cyber-security, in two ways: the CIO must make it an integral part of IT (94%), and the CISO role should be strengthened so that it operates alongside the CIO rather than reporting to the CIO (91%).

In 2017 Signify, for example, centralised all cyber-security management under a chief security officer, including both product and organisational security (supply chain, travel, etc). "I can't look at cyber-security as siloed anymore," says Mr Ramakrishnan.

Mr Ludwig reports to the company's chief technology officer, as do the heads of engineering. He works closely with the heads of products and the CIO, who is responsible for internal systems and core business functions like billing and accounting. "These are my peers," he says. "Together we combine data security governance and implementation."

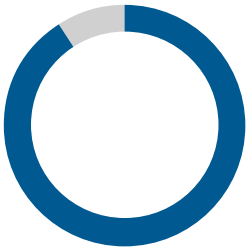
Survey respondents also largely agree (91%) that their organisation needs to better understand which cyber-security measures work best—their focus needs to shift from quantity to quality. While threats from vendors and other third parties have long been a concern, for example, companies may need to focus more on those arising from authorised individuals' personal contacts, such as friends and even family members, and from former employees.

Accordingly, engaging with employees, contractors and other parties is crucial to reducing people-based threats, because the company can never control everything that happens within its network. Rather than simply making rules, periodically updating and informing users, the company needs to monitor its people and work with them so that they understand and are motivated to follow best practices.

At Delta, to keep cyber-security issues from developing among its vendors, "our goal is to work with them collaboratively and always let them know what remedial processes we expect of them," says Ms Wheeler.

While following this path will help companies minimise and mitigate the onrush of data-breach threats, they shouldn't expect to relax any time soon. "Companies can't stop innovation. [Signify] always wants to go into new areas of lighting," Mr Ramakrishnan says. "As a huge business, we need to be able to adapt ourselves quickly. To get there, we'll need preventive and detective measures."

The good news about people-centric risks, he adds, is that "typically, humans follow certain routines. That makes prediction possible; somebody will do the same thing over and over again. You can change that behaviour. Some will never change, but that in itself is predictable."



91%

Survey respondents agree that their organisation needs to better understand which cyber-security measures work best—their focus needs to shift from quantity to quality.

The Economist INTELLIGENCE UNIT

LONDON

20 Cabot Square
London, E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
Email: london@eiu.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@eiu.com

NEW YORK

750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@eiu.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@eiu.com

HONG KONG

1301 Cityplaza Four
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@eiu.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@eiu.com