SECURING THE DIGITAL ECONOMY

ca technologies | VERACODE

01

INTRODUCTION

The digital economy is growing at breakneck speed. In 2015, analysis by **Accenture Strategy and Oxford Economics** estimated that it accounted for 22.5 percent of the GDP, forecast to grow to 25 percent by 2020.

But while organizations are actively pursuing digitization projects to transform their businesses, the increased security risk of an application-centric economy has not resulted in a more comprehensive understanding of – or approach to – cybersecurity among business leaders.

Many business leaders still have a limited understanding of the cybersecurity risks to their company. But as adoption of software-led, digital transformation projects increases, it has never been more important for senior management to grasp the extent of the threat.

CA Veracode commissioned the Securing the Digital Economy report to investigate business leaders' pursuit of digital transformation and their understanding of the cybersecurity risks posed by the increased reliance on applications. In addition, the report provides strategic recommendations for effectively engaging the board on the topic of cybersecurity to support IT leaders as they pursue better cybersecurity in their own organizations.

02

BUILDING THE APPLICATION ECONOMY

Digital transformation is hot on business leaders' agendas. Organizations are pursuing these projects as a means of generating new revenue streams, driving greater efficiencies in existing business operations, and improving the employee and customer experience.

Nearly a third (29 percent) of survey respondents indicated that they are actively pursuing digital transformation projects. A further 29 percent stated that they are either planning for or considering digital transformation projects for the future.

Software is fuelling the growth of this digital economy, underpinning the transformative projects that are driving new revenue streams and greater operational efficiencies.

Of those business leaders that are actively pursuing, planning or considering digital transformation projects, nearly three-quarters of American and German business leaders (both at 73 percent) report their company's budget for software implementation has increased over the past three years to support current and/or future digital transformation projects. This figure is slightly lower in the UK at 67 percent.

The split between where software is being created to drive these initiatives is divided quite evenly. Thirty-seven percent of business leaders reported that either all or most of their software is built internally, compared with 41 percent who indicated that all or most of their software is either built by third-party providers or purchased as commercial off-the-shelf applications.

ONE IN FIVE

business leaders indicated that their software budget had increased 50 percent or more over the past three years

03

UNDERSTANDING THE RISKS

Clearly, digital transformation is no longer a "nice to have" for many businesses. With major digital disruption occurring across all industries, digitizing services and operations is now a crucial component of many companies' strategies for maintaining their customers, reputation and market share.

However, while organizations are becoming increasingly reliant on applications and online services, many business leaders don't understand the plethora of threats that this software-led approach presents, nor how their company would defend against them. In fact, just half of business leaders surveyed fully understand the risk that vulnerable software as a whole poses to their business.

Consider, for example, open source component use. Software is often built with elements of existing code that are taken from online repositories, which enables developers to work faster.

In fact, the applications scanned by Veracode have an average of 46 unique components.

However, this code is often unvetted and, as a result, security flaws found in common components can lead to a vast number of organizations being at risk of exploitation.

For example, the latest State of Software Security report (SoSS), based on application security testing data from scans conducted by CA Veracode's base of more than 1,600 customers, found that 88 percent of Java applications have at least one component-based vulnerability. Despite this widespread threat to the software that underpins digital transformation, less than a third (32 percent) of business leaders understand the risk that vulnerable open source components, a key feature of most applications, pose to their organization.

03

ONLY 28%

of business leaders have heard of the Equifax mega-beach

Struts-Shock

A critical vulnerability identified in the Apache Struts 2 library, Struts-Shock enables remote code execution (RCE) attacks using command injection, for which as many as 35 million sites were vulnerable. Malicious actors exploited the vulnerability in a range of victims' applications, most notably the Canada Revenue Agency and the University of Delaware, in a breach of records that **USA Today reported** could cost the organization as much as $19 million.

Heartbleed

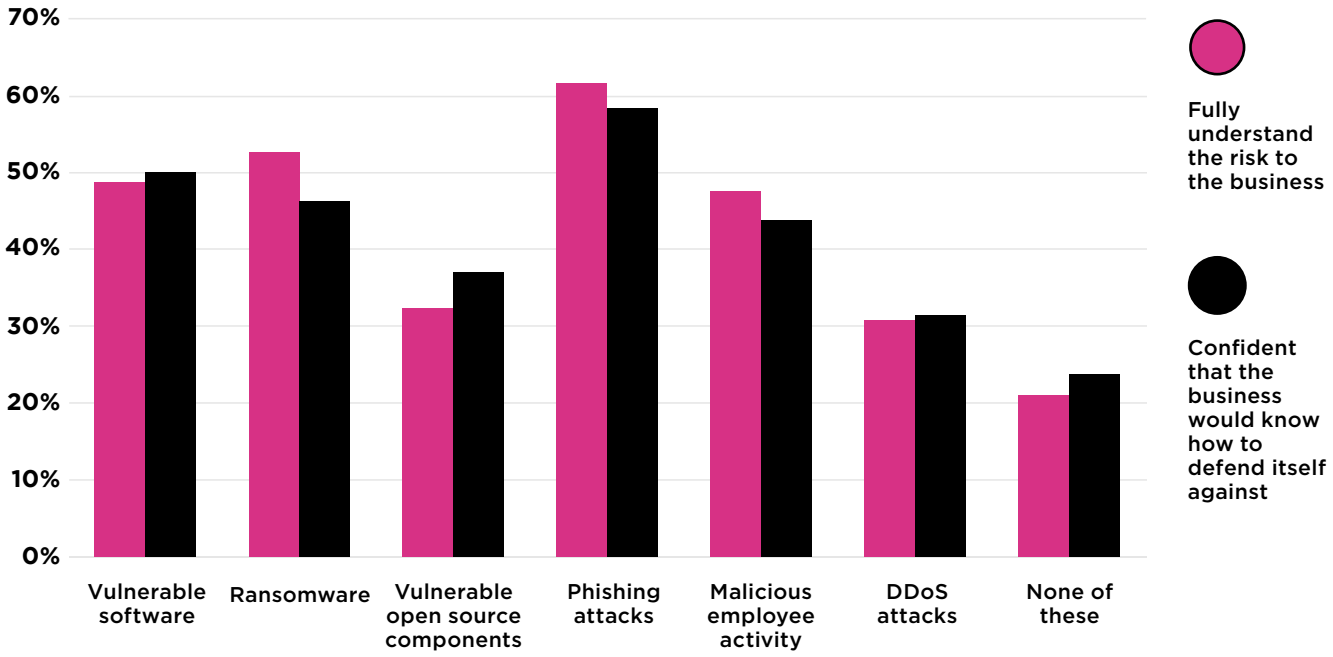
A serious vulnerability found in the popular OpenSSL cryptographic software library. Any server or web site using a vulnerable version of OpenSSL is at risk of having data exposed: including private keys, usernames and passwords, session cookies and other sensitive data from users connecting to the service. It is estimated that up to 20 percent of the websites on the Internet may have been affected by this vulnerability.

The lack of understanding of open source risk is perhaps unsurprising given that, when asked which prominent cyberattacks business leaders had heard of from the previous three years, those caused by vulnerabilities in open source code were among those that were the least recognized. Only 17 percent of business leaders had heard of Heartbleed, while just 8 percent had heard of the Struts-Shock vulnerability.

The low awareness was even true of the 2017 Equifax mega-breach, where the Apache Struts 2 vulnerability was exploited in a web application, which led to a leak of more than 145 million US consumers and 700,000 British customers' personal details. Just 28 percent of business leaders reported having heard of the attack.

Conversely, more than half (58 percent) of all business leaders understand how the threat of ransomware would impact their business. This is perhaps unsurprising after the high number of high-profile attacks led to both 2016 and 2017 being named "the years of ransomware."

03



Brits in particular appear to have woken up to the threat following the two major global ransomware attacks this year. Forty percent of British business leaders have heard of WannaCry, compared with less than a third of American and German business leaders; similarly, 20 percent of Brits have heard of NotPetya, compared with just 12 percent of American and 14 percent of German business leaders.

The greater awareness of these attacks among British business leaders may explain why they are more likely to report that they understand how to protect their organization against ransomware attacks than their US and German counterparts. Fifty-two percent reported that they know how their business would defend itself against such an attack, compared to 45 percent of US and 43 percent of German business leaders.

While there's been a rise in consciousness among some business leaders, a quarter of all business leaders in the UK and US still report not understanding any of the common cybersecurity threats we mentioned. In Germany, this number was slightly lower at 16 percent of business leaders.

When it comes to understanding how to protect their organization against the different cybersecurity threats, a similar number of business leaders from all three countries reported that they didn't know how their business would defend against any of the aforementioned threats (27 percent in the UK, 23 percent in the US and 23 percent in Germany).

04

MAKING THE CHANGE

While a knowledge gap persists across all three regions, we are seeing a shift among many business leaders in their understanding of and approach to cybersecurity.

The constant stream of high-profile attacks has been a catalyst for greater cybersecurity awareness, triggering organizations to rethink their security processes. Nearly one in 10 business leaders, for example, stated that WannaCry had led their organization to rethink its approach to cybersecurity.

US business leaders, in particular, were heavily influenced by recent events. The 2014 Target breach, the 2014 JP Morgan Chase breach, the Yahoo! data breach, and the Apache Struts2 vulnerability, which reportedly caused the 2017 Equifax data breach, were all cited by one in 10 US business leaders as cases that had caused their organizations to rethink cybersecurity.

The risk posed by vulnerabilities in software and devices was clearly exposed by recent events. Of those organizations prompted by cyberattacks on other companies to rethink their own approach to cybersecurity, nearly half of business leaders (47 percent) reported that their organization discussed updating outdated operating systems and conducting more regular scanning for vulnerabilities in software.

These discussions have resulted in direct action by over a third of business leaders, who indicated that the plan to update outdated operating systems and instigate more regular scanning for vulnerabilities in software has either already been implemented or will commence in the next 12 months (34 percent and 37 percent).

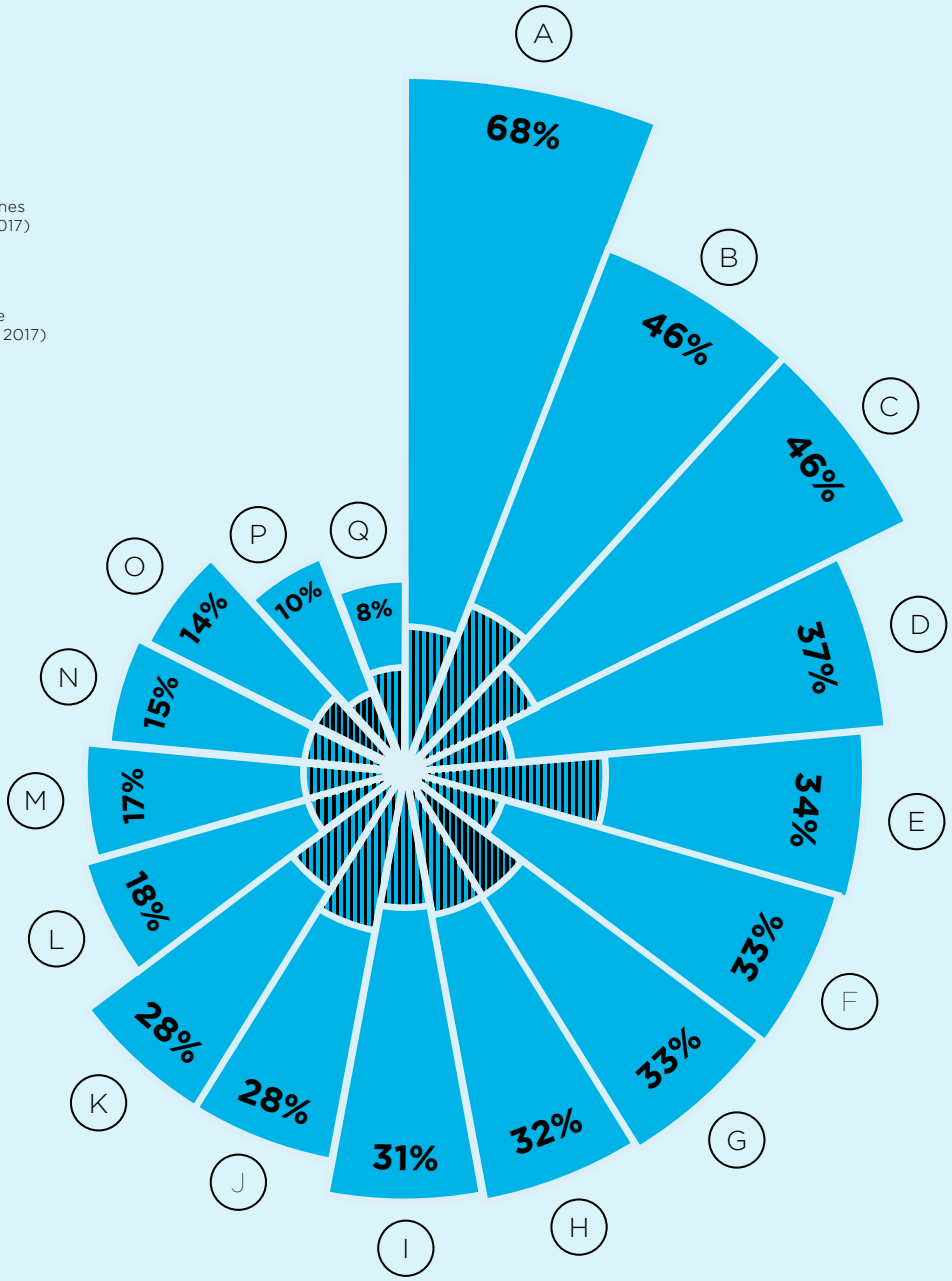
A third of business leaders also discussed setting security thresholds for software built by third-party providers as a result of witnessing high-profile cyberattacks. In the US and Germany, a similar number (31 percent) also discussed setting such thresholds for all commercial off-the-shelf applications.

MAKING THE HEADLINES

Before taking this survey, which, if any, of the following cyberattacks had you heard of?

Which, if any, of the following cyberattacks led your current business to rethink its approach to cybersecurity?

- A Exposure of Hilary Clinton's emails (October 2016)
- B Yahoo! data breach (December 2016)
- C Wikileaks publishing the CIA's Vault 7 hacking tools (March 2017)
- D HBO data breach and leaks of Game of Thrones and other unrealised TV episodes (August 2017)
- E WannaCry ransomware attack (May 2017)
- F Emmanuel Macron's leaked emails during the French presidential campaign (May and July 2017)
- G Exposure of 198 million US voter records on unprotected Amazon s3 server (June 2017)
- H Target breach (December 2013)
- I eBay data breach (May 2014)
- J JP Morgan Chase breach (July 2014)
- K Apache Struts2/ Equifax data breach (September 2017)
- L US Office of Personnel Management breach (2014 and 2015)
- M Heartbleed (April 2014)
- N NotPetya ransomware attack (June 2017)
- O Dyn DDoS attack (October 2016)
- P Cloudbleed (February 2017)
- Q Struts-shock vulnerability (March 2017)



05

TRAINING TACTICS

However, the shift to establish minimum security standards for software hasn't converted into providing in-house developers with the necessary training to develop secure applications. Just one-tenth of business leaders indicated that they will be introducing mandatory training for developers on secure coding in the next 12 months.

The 2017 SoSS report found that 65 percent of all internally developed applications did not pass the OWASP Top 10 policy, the widely accepted standard for application security, upon first scan. The low pass rate on previously untested software has stagnated over the past three years (63 percent in 2015 and 61.1 percent in 2016), highlighting both the importance of application security throughout the development processes, and the fact that developers are consistently introducing the same types of security flaws into code.

However, there is massive potential for organizations that invest in security training for developers. This year's SoSS data reveals that when employers provide developers with opportunities to learn about application security through eLearning subscriptions, they stand to make a 19 percent improvement in fix rates.

Yet, cybersecurity training for employees is not a top priority for business leaders, with just 17 percent planning to introduce mandatory eLearning classes for employees that explain different cybersecurity risks.

However, despite this lack of investment in security education from the business, one-fifth of business leaders indicated that they would be introducing cybersecurity behaviour policies and guidelines in the next 12 months. A further 18 percent stated that they plan to implement cybersecurity best practices into the company's HR policy. A number of businesses are, it appears, putting the responsibility on their employees to maintain good cybersecurity practices without the training that will enable them to deliver on these expectations.

06

ENGAGING THE BOARD ON CYBERSECURITY

Business leaders are resoundingly confident in their IT leaders' ability to secure their company against different cyber threats – nearly three-quarters of business leaders said they have confidence in their IT leaders (75 percent in US, 72 percent in UK and 69 percent in Germany).

However, while business leaders trust their IT leaders to protect their organization against cyberattacks, it doesn't mean that CIOs and IT leaders have an easy job of persuading board members to engage with the topic.

Of those we surveyed, one-third of British and German business leaders reported that their businesses do not plan to take any steps to improve overall cybersecurity in the next 12 months. In the US, this figure is lower at 24 percent.

Digital transformation projects often significantly expand an organization's threat surface area. And as the threat to businesses increases, it's never been more important to engage the board on the topic to ensure that they understand the risk that different cyberattacks pose and the steps the company needs to take to combat against them. This is no easy feat for many IT leaders.

ONE-THIRD

of British and German business leaders reported that their businesses do not plan to take any steps to improve overall cybersecurity in the next 12 months

06

45%

of UK business leaders state that highlighting the cost of a breach, determined by a standard metric and cost of past breaches, will engage the board

So what do business leaders suggest to help IT leaders encourage board members to engage with the topic? Business leaders recommended the following approaches:

Money Matters

Money speaks the loudest in the UK and US, with 45 percent and 46 percent of business leaders stating that highlighting the cost of a breach, determined by a standard metric and cost of past breaches, will engage the board. This is compared with less than a third of survey respondents in Germany at 32 percent.

"Know your audience when speaking to the board about security. Do not use acronyms — think "denial of service" not DDoS. Use visuals instead of text, use analogies, and always use numbers, especially dollars if possible, such as losses from public data breaches. Bottom line: They want to know what are the odds our company will experience a damaging security breach and what are we doing to prevent that."

Chris Wysopal, CTO, Veracode

Personal Brand Damage

Over a third of business leaders (38 percent) reported that giving senior executives examples of the personal brand damage that can come as a result of a data breach is an effective strategy for engaging them with cybersecurity.

This is perhaps unsurprising given that over two-thirds of business leaders we surveyed had heard of the Clinton email hack, which caused significant damage to her personal brand during the election campaign. In fact, it was the most well-known attack of the high-profile attacks that we listed.

Highlighting the threat to executive jobs was also a commonly shared suggestion, with 35 percent of business leaders across all regions suggesting this would get board members sitting up and listening.

06

35%

of business leaders say the threat to executive jobs will get the board to sit up and listen

"We're increasingly seeing CEOs and other executives paying the price after their organization falls victim to severe cyberattacks. And ultimately, this is merely an extension of expectations on the C-Suite when responding to serious events. If CEOs violate environmental, health, or safety standards, they can be fined and even jailed in many countries.

Perfect security is not possible, but with data about our entire lives now being stored and processed by businesses, it is essential that employees and customers alike are afforded a certain standard of cybersecurity. And when such standards aren't met, there ought to be accountability at a senior level."

Paul Farrington, Manager, EMEA Solution Architects at Veracode

Data Regulations

Despite the media hype around GDPR and the potential penalties for organizations that face data breaches after its enforcement, the impact of new data regulations, such as the **EU GDPR** and **New York DFS cybersecurity regulations**, were considered a good tactic for garnering board support by just over a third of UK business leaders. It was recommended as a way to engage the board with cybersecurity by only 28 percent of US and 24 percent of German business leaders.

06

NEARLY HALF

of business leaders state that none of the high-profile cyberattacks had caused them to rethink their approach to cybersecurity

"With the risk of severe penalties added to the already serious consequences of a cyberattack, new data regulations like GDPR can be an effective way of creating a sense of urgency and determining a minimum standard for an organisation's cyber defences.

However, the challenge that many IT leaders may still face is engaging the board with the data regulations to begin with!"

Julian Totzek-Hallhuber, Solution Architect, Veracode

Learnings From High-Profile Cyberattacks

Our findings have already shown how other cyberattacks can be effective in leading organizations to make positive steps to improve their cybersecurity, and just over a third of business leaders across all regions reported that examples of large-scale cyberattacks are effective in demonstrating a similar risk to their organizations.

However, with nearly half of business leaders we surveyed stating that none of the high-profile cyberattacks we highlighted had caused them to rethink their approach to cybersecurity, it is clearly important how IT leaders articulate the way the threat could impact their organization, rather than just relying on the business leaders' knowledge of the story.

"What we saw with recent highly destructive attacks like WannaCry is that they do a lot of damage in a short period of time, so a strategy of "detect it and contain it as quickly as possible" will not be effective. The damage is already done. You also have to take into account what you can do preventatively to make yourself more resilient to these types of attack vectors."

Sam King, SVP and General Manager, Veracode

07

CONCLUSION

Software development and purchasing is booming in many businesses as they pursue digital transformation projects to deliver greater efficiencies, innovation and growth. However, it is clear that business leaders' understanding of the cyber risk hasn't increased at the same rate as their investment in software.

Despite news of major disruption and data breaches frequently splashed across the headlines, understanding of common cyberattacks is worryingly low among business leaders.

It is important that IT leaders leverage the trust they've achieved to help bridge this disconnect. Greater awareness of cybersecurity threats and the appropriate action that must be taken to defend against them will be crucial to ensure that the important investment in digital transformation projects isn't undone by cybercriminals.

Methodology

CA Veracode commissioned YouGov to survey 1,043 business leaders across the UK, US and Germany about their company's digital transformation initiatives and understanding of cybersecurity. The polling was conducted over a nine-day period between 25 September and 4 October 2017.