TUGBOAT LOGIC
by OneTrust

GUIDE

The Future of Information Security

“The world’s most valuable resource is no longer oil, but data.”

THE ECONOMIST

Contents

Introduction

Unless your business has a dedicated security team, chances are you don't think about your information security (InfoSec) program until you need to. In our experience, there are two situations where InfoSec takes center stage. The first, when a prospect requires security assurance before they'll do business with you. The second, when your business is hacked.

Today, there are plenty of reasons to keep InfoSec top of mind. Ever since COVID-19 forced businesses around the world to close their doors and operate remotely, hackers have been exploiting a host of new security vulnerabilities.

TrustRadius, a review site for business technology, recently published a report, which found that 85 percent of B2B vendors said they were honest throughout the sales process. By contrast, only 36 percent of B2B buyers believed that their vendors were giving them the full picture.[1]

This disconnect between vendors and buyers is problematic because buyers are twice as likely to be influenced by vendors they consider to be transparent and trustworthy.

So closing the trust gap is critical. And that's where your InfoSec program can make a big impact. By demonstrating that your business has the right security measures in place, you can establish credibility, build trust and cultivate profitable business relationships.

DID YOU KNOW?

85% of B2B vendors claim they are transparent during the sales process. Only 36% of B2B buyers believe their vendors give them the full picture.

FUN FACT

Customers are twice as likely to work with vendors they consider trustworthy.

[1] Ellett, J. B2B buyers don't trust vendors – and that is a huge opportunity for marketers. Forbes. October 10, 2018.

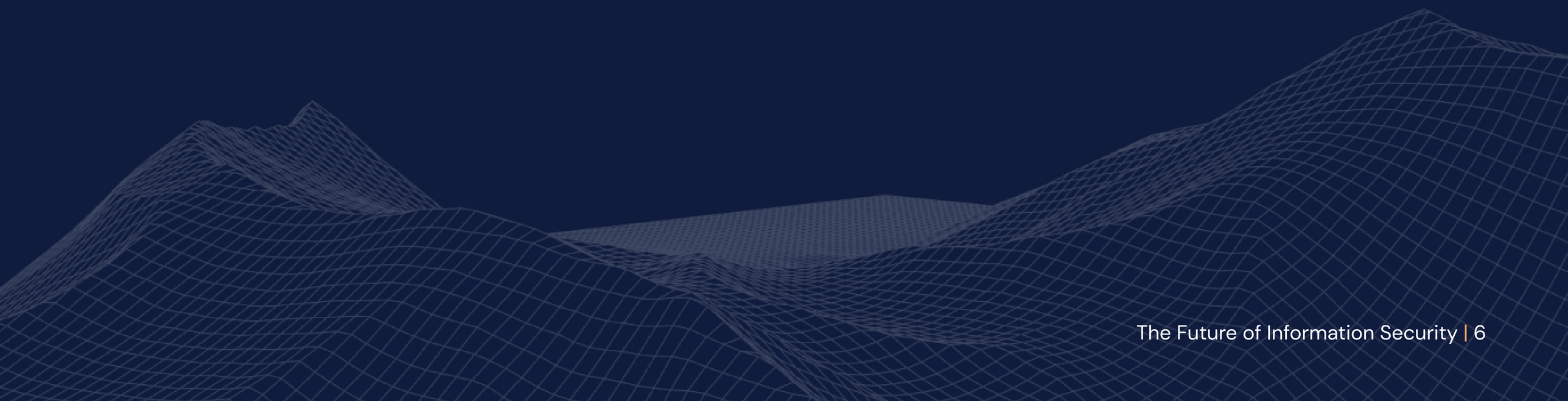
In this eBook, you'll learn how to re-think your approach to InfoSec and apply security best practices without:

→ Revamping your security protocols and procedures.
→ Spending an arm and a leg on your InfoSec program.

Welcome to the future of information security.

THE OLD WORLD APPROACH

Reactive Security



Security Programs Were an Afterthought

"Out with the old, in with the new." – Anon

Few sayings have more relevance to InfoSec than this one. Before 2020, businesses generally viewed InfoSec as a nice-to-have. So, by and large, they adopted a reactive approach to security threats.

In 2019, a KPMG report found that "only a handful of best-in-class businesses are fully integrating cybersecurity into their business transformation agendas from the outset, building digital products and services that meet both the functional and security expectations of consumers. "The remainder typically attempt to retrofit security endeavors to already-established or near-complete transformation outcomes. Friction is inevitably created when security requirements are added at a late stage, delaying or even halting delivery of digital transformation objectives."[2]

Let's take Facebook, for example. In 2018, hackers exploited a security flaw in the platform's infrastructure, which gave them access to personal data of at least 50 million users.

The social media juggernaut took some flak from security and risk experts such as Jeff Pollard, vice president and principal analyst at Forrester, who said the fact that Facebook stored so much data meant that it should have been prepared for such attacks.[4] For Pollard, Facebook shouldn't have been playing catch up.

DID YOU KNOW?

55% of small- and medium-sized businesses experienced a cyberattack in the last year?[3]

FAST FACT

37 billion customer records were exposed last year alone from data breaches—the highest number of exposures since 2005.[5]

[2] *Consumer loss barometer: The economics of trust.* KPMG. 2019. [3] Williams, Mark. *Infographic: 10 statistics that show why training is the key to good data protection and cybersecurity.* pensar. May 15, 2018. [4] Lee, Dave. Facebook security breach: Up to 50m accounts attacked. BBC News. September 29, 2018. [5] Whitney, Lance. 2020 sees huge increase in records exposed in data breaches. TechRepublic. January 21, 2o21.

Security Programs Were All or Nothing

But being prepared didn't mean Facebook needed 100 percent ironclad security.

According to KPMG, one of the most common cybersecurity mistakes businesses make is to believe that they must achieve 100 percent security, which is neither feasible nor appropriate.[6] For instance, airlines claim that flight safety is their highest priority, but they also acknowledge the inherent risk of flying.

So it is with cybersecurity.

The reality is that all businesses great and small, public and private, famous and obscure should assume that, at some stage, their information systems will be attacked. And it's this assumption that Facebook should have made, which would have changed its security posture from a reactive stance to a proactive one.

Heather Adkins, director of information security at Google, believes security teams should spend less time on the impossible task of creating unhackable products and devote more time to building out their response plans for when the inevitable happens. "At some point in the history of your company, you're probably going to get hacked," she says. "The question is not whether or not you're going to get hacked, but are you ready?"[7]

QUOTABLE QUOTE

"The question is not whether or not you're going to get hacked, but are you ready?"

HEATHER ADKINS
DIRECTOR OF INFORMATION SECURITY | GOOGLE

[6] *Cyber security: It's not just about technology. KPMG. 2014.*
[7] Holmes, Aaron. *Cybersecurity power players: Meet the top execs tasked with protecting the secrets of the world's biggest tech companies.* Insider. February 25, 2021.

Security Programs Were a Means to an End

In the old world, security programs were off-the-shelf and weren't molded to fit specific products and services.

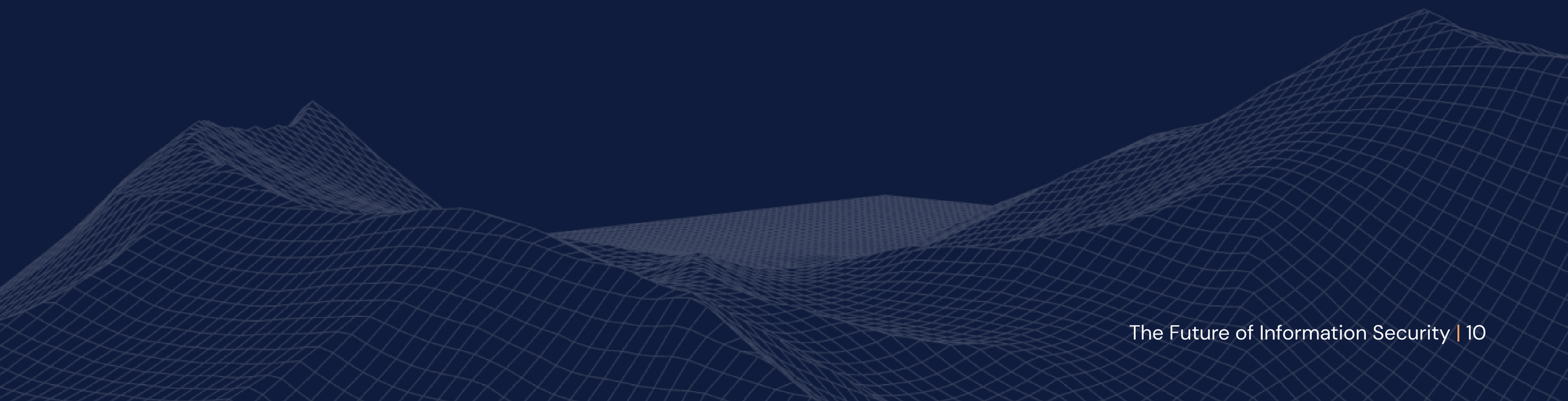
As for security compliance, it was simply a tick-box exercise designed to satisfy a laundry list of industry regulations. It was a process that companies endured rather than engaged with in order to do business.

But with the heightened security implications of businesses migrating their data en masse from physical servers to the cloud, viewing compliance as a tick-box exercise just won't cut the mustard anymore.

Today, it's a vital operational risk, which calls for the immediate and undivided attention of your company's leadership and senior management team.

NEW MARKET REALITY

The Trust Crisis



The Call for Proactive InfoSec

Change begets change.

As digital becomes the norm in the 'new world,' the role of InfoSec needs to change, too, in order to facilitate agile adoption, experimentation and implementation of technology.

InfoSec that remains reactive isn't fit for purpose in the era of digital transformation. As cybersecurity threats grow in volume and sophistication, companies that enjoy success in today's market are those that build trust into their digital products and services by proactively investing in InfoSec.

This investment takes place against a backdrop of new, COVID-19-induced or accelerated market realities (some of which may remain long after COVID has gone).

Here are the main ones:

→ Increased cloud migration: Since the onset of COVID, traditional brick-and-mortar businesses have started altering their IT strategies to move a growing share of their digital assets such as data, workloads, resources and applications from on-premises data centers to the cloud.

FAST FACT

40% of companies lack an information security policy.[8]

[8] protiviti. *Managing the Crown Jewels and Other Critical Data.* protiviti. Accessed January 25, 2021.

The Call for Proactive InfoSec

→ Increased remote working: COVID has also seen IT teams implement changes enabling people to work from home. Due to below par technological infrastructure and inadequate data security, this mode of working has become a Pandora's Box of new forms of information theft—representing an increased cybersecurity risk to businesses.

→ Increased automation: Businesses across various sectors have expedited their use of robots, chatbots and autonomous vehicles to provide contactless care to patients, monitor grocery stock levels and connect the elderly to their loved ones.

→ Increased adoption of low-density offices: For workers who have returned to the office, businesses are adhering to social distancing requirements by designing low-density floor plans with less assigned space and more space for collaborative activities.

→ Increased online activity: The coronavirus pandemic has caused a global spike in the use of digital technology due to nationwide lockdowns and social distancing rules. People routinely opt for telemedicine to see a doctor, use video conferencing apps to talk with friends and family and watch streaming services for entertainment.

Building Trust With Your InfoSec Program

According to an article published in the Harvard Business Review, businesses today are selling more than products and services. They're selling trust.[6]

Trust is the biggest factor in buying decisions. A loss of trust can result in a trust crisis, causing customers to completely abandon a product or the company that made it. Trustworthiness also determines which vendors a company will do business with or steer clear of. This observation holds true for both the B2C and B2B spaces.[7]

Customers' increasing dependence on software in almost every area of their personal and professional lives coupled with the intrinsic privacy and security vulnerabilities connected to software itself, means that your InfoSec program must do three things to earn your customers' trust:

- → Prioritize customer data privacy and security.
- → Demonstrate these priorities by getting compliant with the right standards and regulations and maintaining continuous compliance.
- → Provide security assurance by being transparent about the scope and capabilities of your InfoSec program.

DID YOU KNOW?

4000 companies lost out on $180 billion in revenue because of trust, according to Accenture's 2018 Competitive Agility Index.

[6] *Cyber security: It's not just about technology*. KPMG. 2014.
[7] *Half of Companies on the Accenture Competitive Agility Index Experienced a Major Drop in Trust, Losing Out on $180B in Potential Revenues*. Accenture. October 30, 2018.

The True Costs of Losing Customer Trust: TalkTalk and Equifax

When customer trust is lost, the financial consequences can be hard-hitting.

Hop across the pond to the UK and you'll find that TalkTalk is its fourth largest broadband company.

In 2015, TalkTalk's systems were hacked and the personal information of nearly 160,000 customers was accessed including names, phone numbers, email addresses and even bank account details. This resulted in the B2C company's profits being slashed by more than 50 percent—from £32 million ($44 million) to £14 million ($19 million).[8]

Sometimes, the cost of losing trust is that customers vote with their feet.

Right here in the US, Equifax is one of our three largest credit reference agencies. Although it's primarily a B2B company, the Atlanta-based firm suffered a data breach in 2017 that compromised the sensitive data of 145.5 million consumers.

The Equifax breach was termed "one of the worst ever"[9]—not only by its reach, but also by the kind of information exposed to the public, which included social security numbers, addresses and the numbers of some driver's licenses. Beyond its financial cost, the security breach had "prompted some customers to hold back business."[10]

[8] *TalkTalk profits halve after cyber attack. BBC News. May 12, 2016.*
[9] Fiegerman, Seth. *The biggest data breaches ever.* CNN. September 7, 2017.
[10] McCrank, John. *Equifax profits fall as hacking costs takes toll.* Reuters. November 10, 2017.

The True Costs of Losing Customer Trust: TalkTalk and Equifax

In the new world, trust is foundational to building high-quality, long-term customer relationships, which typically yield customer loyalty and high customer lifetime value.

If businesses continue to perform reactive security manoeuvres, which don't instil confidence in their customers, the likelihood is they will only enjoy one-off, transactional relationships at best. As such, these businesses will probably miss out on the financial rewards that would have come their way if they had been more proactive in safeguarding their customers' security.

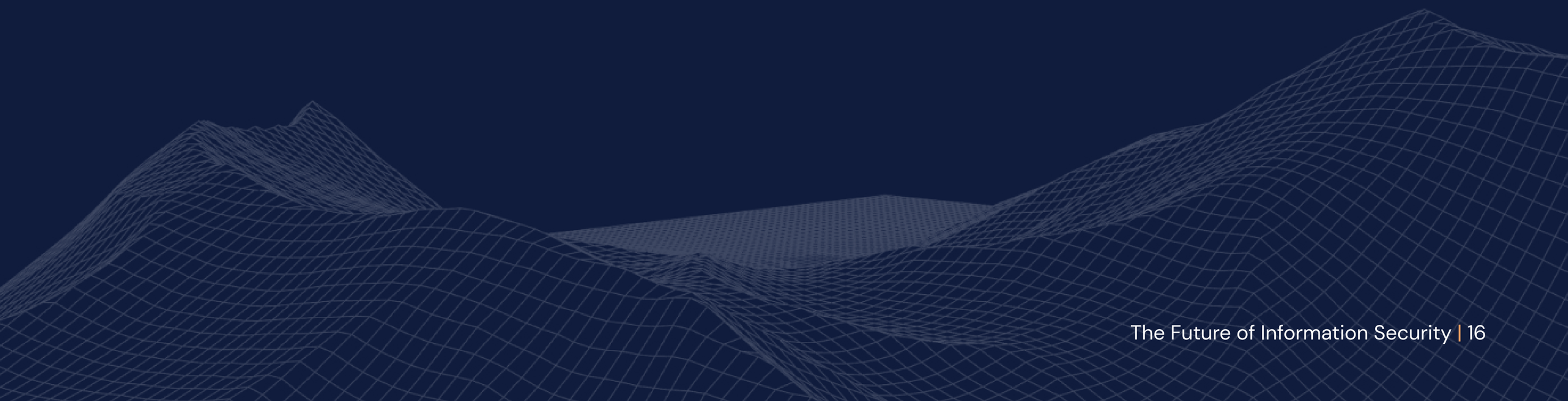
FAST FACT

The Equifax data breach cost the company $1.38 billion.[11]

[11] Vijayan, Jai. 2017 Data Breach Will Cost Equifax at Least $1.38 Billion. Dark Reading. January 15, 2020.

MARKET RESPONSE

A New Security Landscape



Regulations, Security Frameworks and New Business Practices

The market response to the trust crisis has been threefold:

→ Increase in regulations: To cater to the new market reality in which businesses are collecting more data than ever before (including personally identifiable information), some governments have introduced wide-ranging data privacy legislation. These laws govern how businesses collect and use personal information. Recent examples include:

- → The General Data Protection Regulation (GDPR) in the European Union.
- → The California Consumer Privacy Act (CCPA) in the US.
- → The Personal Information Protection and Electronics Documents Act (PIPEDA) in Canada.

Right now, there are no international regulations guaranteeing data protection and security, although there are reportedly talks of a global GDPR on the horizon. Facebook and Snap have called for "effective privacy and data protection" as part of a "globally harmonized framework."[12]

DID YOU KNOW?

Last year alone, 12 new cybersecurity laws were passed in the U.S[13]

[12] *Facebook and Snap Inc call for a GDPR-aligned Australian Privacy Act.* Stimulus Check Up. Stimulus Check Up. Feb 8, 2021.
[13] Brumfield, Cynthia. *2020 outlook for cybersecurity legislation.* CSO Online. January 6, 2020.

Regulations, Security Frameworks and New Business Practices

→ Increased involvement of third-party security and assurance bodies: Arguably, the two leading InfoSec assurance standards are SOC 2 and ISO 27001. Organizations that independently vet business security programs for customers and provide them with proof of compliance are growing in popularity, such as the American Institute of Certified Public Accountants (AICPA), which handles SOC 2 in the US and the ANSI-ASQ National Accreditation Board (ANAB), which deals with ISO 27001 in the UK.

→ Increased self-regulation by software firms: In an effort to improve web privacy, software companies have taken it upon themselves to ban third-party cookies by default. Google is the latest to announce such plans.[14] The software giant follows in the footsteps of Mozilla, Safari and privacy-focused browsers, such as Tor and Brave.

FAST FACT

A Tenable survey found that 35% of organizations have adopted the ISO 27001 security framework.[15]

[14] Graham, Megan. *Google says it won't use new ways of tracking you as it phases out browser cookies for ads*. CNBC. March 3, 2019.
[15] Watson, Emily. *Top 4 cybersecurity frameworks*. IT Governance. January 17, 2019.

The Case for Proactive Security: FireEye

The steps taken by the market to avert the trust crisis confer the following benefits on customers:

- → They provide online protection.
- → They provide an objective yardstick with which to assess whether or not it is safe and secure to work with a particular business.
- → They provide a showing of good faith (for instance, the Google self-regulation example).

But as well-intentioned as these measures may be, they're still reactive.

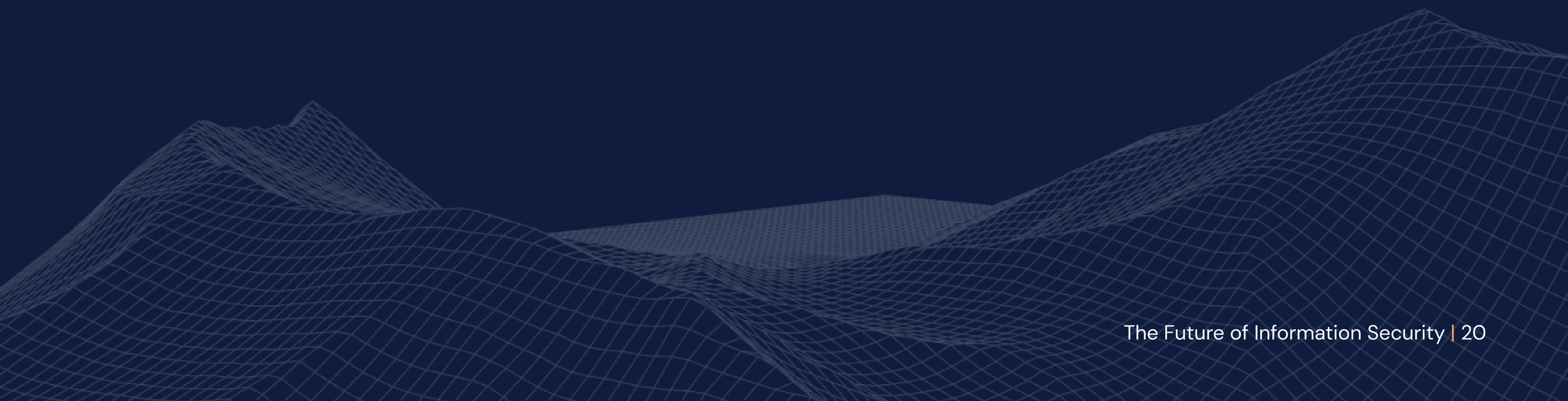
For instance, FireEye is one of the largest cybersecurity companies in the US. Despite its size, stature and notoriety, the firm was hacked in 2020.[16]

The incident is considered "among the most significant breaches in recent memory" and underscores the difficulty that even cybersecurity companies have warding off motivated and determined hackers when attempting to do so from a reactive position.

[16] Bing, Christopher. and Menn, Joseph. *U.S. cybersecurity firm FireEye discloses breach, theft of hacking tools*. Reuters. December 9, 2020.

THE NEW WORLD APPROACH

Proactive Security



The Anatomy of an Infosec Program for the Modern Era

By now, it's probably becoming clear that, if the InfoSec program of the new world is to achieve different results to its predecessor in the old world, it will call for something to be done differently—namely, businesses taking a proactive approach to security.
So, here's the anatomy of an InfoSec program fit for 2021 and beyond.
An InfoSec program, which is designed to accommodate the market realities of the new world, consists of six main themes:

1. InfoSec assumes that a cyber attack or security breach is inevitable. The new world view of InfoSec makes a single assumption—that irrespective of how tight its security protocols may be, your business will be hacked at one time or another.

2. InfoSec is a must-have for businesses. It's no longer a luxury, but a necessity for your business to have a comprehensive InfoSec program.

3. InfoSec must be proactive. Anticipatory security, rather than reactionary security, is now the order of the day.

4. InfoSec must be product-specific. Generic security programs must be substituted with highly bespoke programs, which are tailored to your individual products or services.

CRITICAL KEYWORDS

Continuous compliance is about having the right strategy, tools, people and culture in place to ensure you're always meeting industry regulatory demands and protecting critical data assets.

The Anatomy of an Infosec Program for the Modern Era

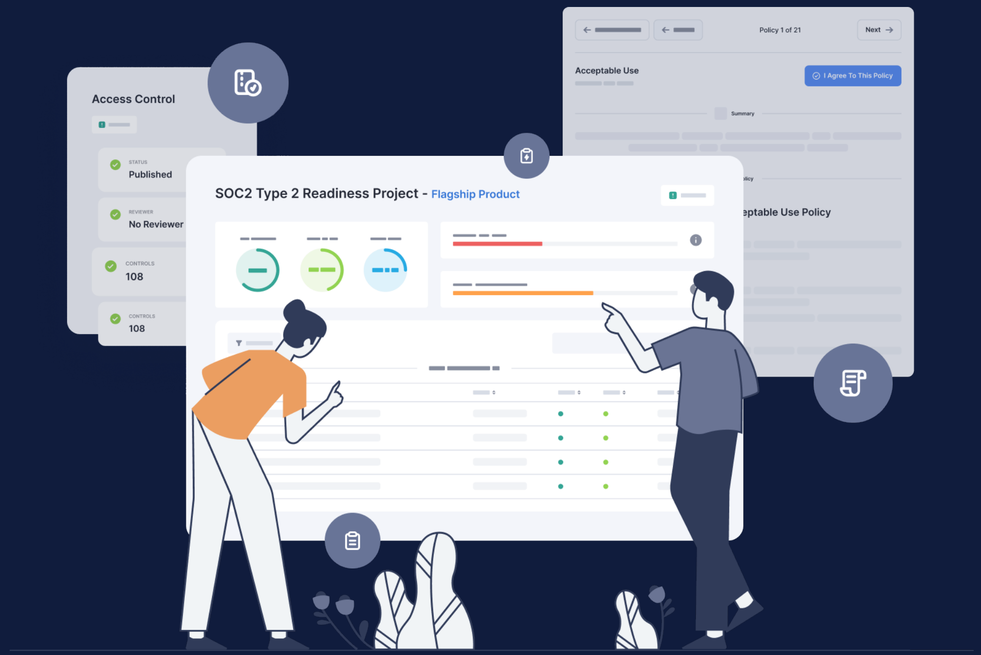
5 InfoSec must be continuously compliant. Your business must always be audit-ready—prepared to document that it's fully compliant with necessary security regulations and frameworks at any given point in time.

6 InfoSec is ultimately about security assurance. Gone are the days of running through a compliance checklist simply to close a deal or satisfy a client's demands. Nowadays, the state of being compliant isn't enough. Businesses must have a system of record for security management, which demonstrates 'security assurance' to your customers—that your business is resilient to threats and vulnerabilities and their trust in you is well-placed.

CRITICAL KEYWORDS

Security assurance comes from the ability to demonstrate your systems meet certain security requirements and are resilient against vulnerabilities and failures. By providing security assurance, you can prove that your business is trustworthy.

Conclusion



Trust is today's currency and a key differentiator for companies that put security assurance at the heart of their business. In PwC's 20th Global CEO Survey, 69 percent of business leaders said it's becoming increasingly difficult to earn and maintain trust in a digital world.[17]

Your business can ease the process of building trust by doing more than what is required by law. One way your business can achieve this is by proactively managing privacy and cybersecurity risks.

The core benefit to your customers is the confidence that your business is collecting, storing and using their personal information safely and securely at all times. The main benefit to your business lies in gaining potential customers for life. The bottom line is that, in today's world, your company should insert privacy and cybersecurity in the center of its business strategy to win customers' hearts, minds and, ultimately, earn their trust.

At Tugboat Logic, we believe privacy and security issues can no longer be an afterthought in the product development cycle—not solely because of the value of your customers' privacy and security, but because of their effect on your business, too.

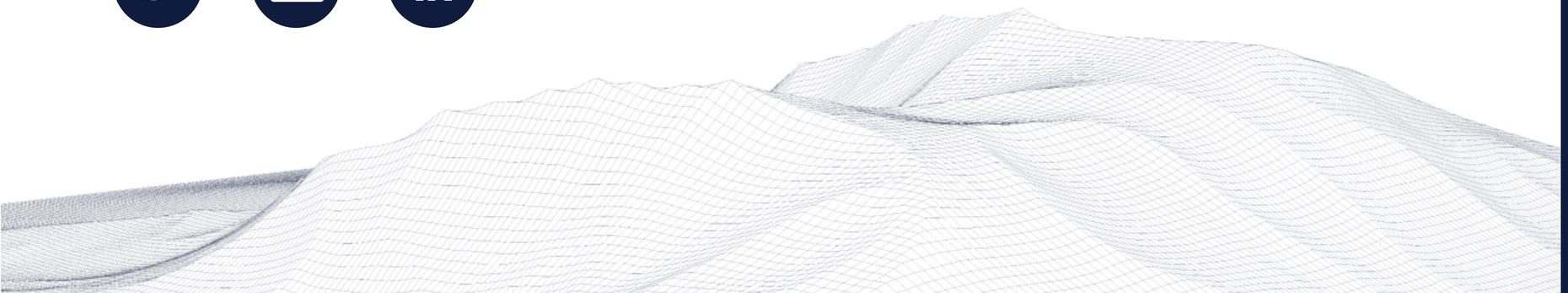
[17] Bing, Christopher. and Menn, Joseph. *U.S. cybersecurity firm FireEye discloses breach, theft of hacking tools.* Reuters. December 9, 2020.

ABOUT TUGBOAT LOGIC

Tugboat Logic is the Security Assurance Platform that provides continuous compliance. It uses automated technology to demystify the process of creating and managing an InfoSec program. With Tugboat Logic, companies can quickly get secure and prove it to customers. Powered by AI, Tugboat Logic's patent-pending technology automates InfoSec policy creation, audit readiness, and security questionnaire response so companies can gain trust with customers and sell more. Tugboat Logic helps businesses prepare for audits in half the time and at a fraction of the cost, ensures they can respond to security questionnaires in minutes (not hours), and builds and scales their InfoSec plan in minutes.

START SELLING MORE TODAY

Interested in turning your security and compliance program into a business advantage?
Get a free trial or contact one of our representatives at info@tugboatlogic.com.



TUGBOAT LOGIC
by OneTrust