# 2019 Forcepoint Cybersecurity Predictions Report

# Introduction

Innovation thrives when people can collaborate in a trusted manner, leveraging data creatively and freely through technology.

Take the commute to work, for example, as it offers a glimpse into the relationship between trust and innovation. Everything a person does in that commute to the office is underpinned by trust: they trust a train to run per the specified timetable, that their barista will not mix up their coffee order. They trust their employer to control access to their CRM SaaS app, to ensure a confidential sales record is not uploaded to a rogue phishing website. And, since trust is established between parties, employers trust employees to protect critical data at all times, with an expectation to remember their cybersecurity training.

***Trusted interactions lead to the creation of value for a company, but the intersection between end-user and data is also the point of greatest vulnerability for an enterprise, and the primary source of breaches driving cyber risk to all-time highs.***

How can security professionals know if an end-user login is the result of an employee's coffee-shop WiFi access or an attacker abusing authorized credentials? How do they know whether a user identity is behaving consistently or erratically on the network compared to an established routine? Knowing and acting on the difference between an individual legitimately trying to get their job done and a compromised identity is the difference between innovation and intellectual property (IP) loss, the difference between an organization's success or failure.

As data and digital experiences are placed into the hands of others, the concept of trust becomes even more crucial. Businesses can rise or fall based on trust—companies abusing their customers' trust face millions or billions of dollars in regulatory fines and lost market value, as in the case of Facebook and Cambridge Analytica.

In the 2019 Forcepoint Cybersecurity Predictions Report, we explore the impact of businesses putting their trust in cloud providers to protect their data, the impact of end-user trust in those securing personal biometric data, the cascading of trust into the supply chain to protect any critical data in their custodianship, and trust in algorithms and analytics successfully piloting automobiles and alerting security professionals to potential data loss incidents.

Our global Security Labs, Innovation Labs, CTO, and CISO teams have put forward their top predictions for the year to come. Read on to discover their seven predictions for 2019. How will you guide your organization through the increasingly complex trust landscape?

01

# The winter of AI?

## Disillusionment sets in as AI and machine learning are held accountable for their claims

***Prediction:***

*There is no real AI in cybersecurity, nor any likelihood for it to develop in 2019.*

**Contributor:**

**Raffael Marty**

*Vice President of Research and Intelligence*

In addition to the myriad of constantly evolving threats in today's landscape, organizations are hampered by an ongoing skills shortage— analysts predict a shortfall of 3.5 million cybersecurity jobs by 2021.[1] In an attempt to fill the void, organizations have turned to the promise of big data, artificial intelligence (AI), and machine learning.

And why not? In other industries, these technologies represent enormous potential. In healthcare, AI opens the door to more accurate diagnoses and less invasive procedures. In a marketing organization, AI enables a better understanding of customer buying trends and improved decision making.[2] In transportation, autonomous vehicles represent a big leap for consumer convenience and safety; revenue from automotive AI is expected to grow from $404 million in 2016 to $14 billion by 2025.[3]

The buzz for cybersecurity AI is palpable. In the past two years, the promise of machine learning and AI has enthralled and attracted marketers and media, with many falling victim to feature misconceptions and muddy product differentiations. In some cases, AI start-ups are concealing just how much human intervention is involved in their product offerings.[4] In others, the incentive to include machine learning-based products is one too compelling to ignore, if for no other reason than to check a box with an intrigued customer base.

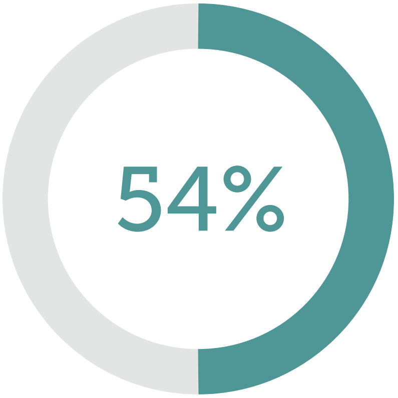
Today, cybersecurity AI in the purest sense is nonexistent, and we predict it will not develop in 2019. While AI is about reproducing cognition, today's solutions are actually more representative of machine learning, requiring humans to upload new training datasets and expert knowledge. Despite increasing analyst efficiency, at this time, this process still requires their inputs—and high-quality inputs at that. If a machine is fed poor data, its results will be equally poor. Machines need significant user feedback to fine-tune their monitoring; without it, analysts cannot extrapolate new conclusions.

On the other hand, machine learning provides clear advantages in outlier detection, much to the benefit of security analytics and SOC operations. Unlike humans, machines can handle billions of security events in a single day, providing clarity around a system's "baseline" or "normal" activity and flagging anything unusual for human review. Analysts can then pinpoint threats sooner through correlation, pattern matching, and anomaly detection. While it may take a SOC analyst several hours to triage a single security alert, a machine can do it in seconds and continue even after business hours.

However, organizations are relying too heavily on these technologies without understanding the risks involved. Algorithms can miss attacks if training information has not been thoroughly scrubbed of anomalous data points and the bias introduced by the environment from which it was collected. In addition, certain algorithms may be too complex to understand what is driving a specific set of anomalies.

Aside from the technology, investment is another troublesome area for cybersecurity AI. Venture capitalists seeding AI firms expect a timely return on investment, but the AI bubble has many experts worried. Michael Woodridge, head of Computer Science at the University of Oxford, has expressed his concern that overhyped "charlatans and snake-oil salesmen" exaggerate AI's progress

*Click above to see Raffael Marty, Vice President of Research and Intelligence, discuss this prediction.*



*Only 1 in 2 (54%) employees belonging to companies with extensive experience in machine learning check for fairness and bias.*[9]

to date.[5] Researchers at Stanford University launched the AI Index, an open, not-for-profit project meant to track activity in AI. In their 2017 report, they state that even AI experts have a hard time understanding and tracking progress across the field.[6]

A slowdown of funding for AI research is imminent, reminiscent of the “AI Winter” of 1969, in which Congress cut funding as results lagged behind lofty expectations.[7] But attacker tactics are not bound by investments, allowing for the continued advancement of AI as a hacker’s tool to spotlight security gaps and steal valuable data.

The gold standard in hacking efficiency, weaponized AI offers attackers unparalleled insight into what, when, and where to strike. In one example, AI-created phishing tweets were found to have a substantially better conversion rate than those created by humans.[8] Artificial attackers are formidable opponents, and we will see the arms race around AI and machine learning continue to build. ■

> ***Today’s AI solutions are not built to deal with ambiguity. Humans, on the other hand, are better able to balance multiple variables and context associated with behavior to make decisions-especially when dealing with the unexpected. The cybersecurity industry can’t avoid dealing with this ambiguity.***
>
> — Audra Simons, Head of Innovation & Prototyping, Forcepoint

**99%** of surveyed Forcepoint customers identified evolving cyber attacks to be an important security issue for their organization.[10]

02

# Industrial IoT disruption at scale

## Attackers seek out vulnerabilities in cloud infrastructure and hardware

***Prediction:***

*Attackers will disrupt Industrial Internet of Things (IIoT) devices using vulnerabilities in cloud infrastructure and hardware.*

**Contributor:**
**George Kamis**
*Chief Technology Officer*
*for Global Governments*
*and Critical Infrastructure*

Networked industrial control systems (ICS) that require "always-on" connectivity represent an expanded attack surface, and nowhere is that more apparent than in IoT devices. WiFi and other network-connected sensors in autonomous vehicles and appliances have introduced a rapidly evolving set of security requirements. While attacks on consumer IoT are prevalent, the possibility of disruption in manufacturing and similar industries makes the threat all the more serious.

The 2018 Forcepoint Cybersecurity Predictions Report discussed the potential for man-in-the-middle (MITM) attacks on IoT networks.[11] In 2019, attackers will break into industrial IoT devices by attacking the underlying cloud infrastructure. This target is more desirable for an attacker— access to the underlying systems of these multi-tenanted, multi-customer environments represents a much bigger payday.

There are three issues at play: the increasing network connectivity to edge computing; the difficulty in securing devices as more compute moves out to the edge, as they do in remote facilities and IoT devices, and the exponential number of devices connecting to the cloud for updates and maintenance.

*Click above to see Carl Leonard, Principal Security Analyst, discuss this prediction.*

81% of surveyed Forcepoint customers identified disruption of IoT to be an important security issue for their organization.[14]

76% of surveyed Forcepoint customers are concerned about the security of IoT devices or infrastructure either within their company or their supply chain.[15]

As control systems continue to evolve, they will be patched, maintained, and managed via cloud service providers. These cloud service providers rely on shared infrastructure, platforms, and applications in order to deliver scalable services to IoT systems. The underlying components of the infrastructure may not offer strong enough isolation for a multi-tenant architecture or multi-customer applications, which can lead to shared technology vulnerabilities. In the case of industrial IoT, a compromise of back-end servers will inevitably cause widespread service outages and bring vital systems to a screeching halt. Manufacturing, energy production, and other vital sectors could be affected simultaneously.

With Meltdown and Spectre in 2018, we saw vulnerabilities that bypass the software and firmware layers to expose processor hardware to exploits. In this scenario, attackers use low-privilege programs in order to access more critical data, such as private files or passwords. Almost all CPUs since 1995 are thought to be vulnerable,[12] and new variants of Spectre continue to surface. Attackers will divert their attention on developing variants that subvert the underlying cloud infrastructure used by IIoT systems. As processor speed is critical to performance, manufacturers and cloud service providers could continue to choose speed over security in order to gain a competitive edge, inadvertently introducing further vulnerabilities.

Organizations will need to move from visibility to control where the IT and OT networks converge to protect against these deliberate, targeted attacks on IIoT systems.

*IoT will be the most challenging area of security. Not many security professionals have had time to focus on IoT and it is becoming the trend in our life. It's consistently getting bigger and bigger, and it can be very dangerous when IoT devices get exploited.* [13]

— Sean Wang, Engineer, Bank of Hope

03

# A counterfeit reflection

## Face recognition software is infiltrated to steal your face

***Prediction:***
*Hackers will game end-user face recognition software, and organizations will respond with behavior-based systems.*

**Contributor:**
**Nico Fischbach**
*Global Chief Technology Officer*

To an attacker, the successful theft of legitimate credentials must feel a bit like winning the lottery. End-users are locked out of their accounts, access to third-party cloud services such as Dropbox and Microsoft Office 365 is cut off, critical data downloaded or wiped entirely. The soaring number of breaches reveal one simple truth: email addresses, passwords, and personal information (favorite color, pet name) are no longer sufficient to protect identities online.

In hijacking an end-user's identity, phishing still reigns supreme, taking first place in a 2017 study conducted by Google, the University of California, Berkeley, and the International Computer Science Institute.[16] From 2016 to 2017, researchers calculated there were more than 12.4 million victims of phishing, advising the hardening of authentication mechanisms to mitigate hijacking.

While credential theft is the oldest (and most effective) trick in the book, it does not mean that attackers are not coming up with new tricks. Two-factor authentication (2FA) adds an extra layer of security, but even this method has a vulnerability: it is usually accomplished through cellular phones.

In 2018, Michael Terpin, a co-founder of the first angel investor group for bitcoin enthusiasts, filed a $224 million lawsuit against a telecommunications company, claiming the loss of $24 million worth of cryptocurrency as a result of a “SIM swap.”[17] Attackers used phishing and social engineering tactics to trick a customer service representative into porting Terpin’s phone number to an untraceable “burner” phone. Once this exchange took place, the crime became as simple as clicking a “Forgot Password?” link.

Moving past 2FA, biometric authentication uses data more unique to each end-user. At first, the possibility of verifying a person’s identity via physiological biometric sensors seemed like a promising alternative to 2FA. Fingerprints, movements, iris recognition—all of these make life difficult for attackers seeking to access resources by stealing someone else’s identity.

But in recent years, even biometric authentication has begun to unravel. In 2016, researchers at Michigan State University uncovered cheap and easy ways to print the image of a fingerprint using just a standard inkjet printer.[18] And in 2017, researchers at New York University’s (NYU) Tandon School of Engineering could match anyone’s fingerprints using digitally altered “masterprints.”[19]

Facial recognition has gone mainstream thanks to Apple’s release of its iPhone X, which uses a flood illuminator, an infrared camera, and a dot projector to measure faces in 3D, a method they claim cannot be fooled by photos, videos, or any other kind of 2D medium.[20] But the reality is that facial recognition has serious vulnerabilities—and that is why we think hackers will steal the public’s faces in 2019. In fact, it has already happened, albeit only at the behest of researchers. In 2016, security and computer vision specialists from the University of North Carolina defeated facial recognition systems using publicly available digital photos from social media and search engines in conjunction with mobile VR technology.[21]

While passwords may change, physical biometrics are genetic and specific to each person. By the same token, behavioral biometrics provide a continuous authentication layer by incorporating a person’s physical actions, including keystroke, mouse movement, scroll speed, how they

*Click above to see Nico Fischbach, Global Chief Technology Officer, discuss this prediction.*

toggle between fields, as well as how they manipulate their phone based on the accelerometer and gyroscope.[22] It is simply impossible for imposters to mimic these actions.

The combination of behavioral biometrics with strong authentication, either based on advanced technology like FaceID or 2FA, is a more sensible approach. Organizations can identify intruders who hijack open-work with at-login and in-use/continuous authentication, paving the way for risk-based approaches to trigger authentication checkpoints when risk levels rise.[23] ■

> ***Social engineering is my biggest concern, as many users still tend to be unaware of those kinds of attacks, and are easily duped.[24]***
>
> — David Timmins, Server Administrator, Daystar Television Network

04

# Courtroom face-off

## Insider threats result in a litigious blame game

***Prediction:***
*2019 will see a court case in which, after a data breach, an employee claims innocence and an employer claims deliberate action.*

**Contributor:**
**Marlene Connolly**
*Group Counsel and Senior Director*

Data protection regulations have bolstered an employee's ability to claim foul when a data breach occurs in the workplace, especially when it results in the exposure of their personally identifiable information (PII).[25] But what happens when an employer sues an employee on grounds they purposefully stole data or caused a breach?

We believe that 2019 will see a court case where, after a data breach, an employee claims innocence and an employer claims deliberate action.

This should not be confused with rampant negligence, as in a recent study where a staggering 24 percent of UK employees admitted to sharing confidential business information.[26] Even elected officials have openly discussed sharing work computer passwords with staffers.[27] Although many incidents are classified as accidental, those resulting from malicious intent cause more breaches. Theft, the use of malware, or unauthorized access are still three times more likely to be categorized as a data breach than unintentional or inadvertent incidents.[28]

*Click above to see Audra Simons, Head of Innovation and Prototyping, discuss this prediction.*

83% of surveyed Forcepoint customers identified GDPR and other regulations to be an important security concern for their organization.[33]

On June 20, 2018, a lawsuit was filed against Martin Tripp, an ex-Tesla employee who, according to courtroom documents, collected and leaked data in an attempt to warn investors and the public about allegedly misleading production reports and faulty battery modules installed in Tesla cars.[29] Tesla refuted Tripp's claims, stating it was poor job performance and an eventual reassignment that led Tripp to industrial sabotage. Tripp installed software that would continue to collect data even after he left the company, and exposed confidential photos and a video of Tesla's manufacturing system.

Whether Martin Tripp is a saboteur or whistleblower is still to be determined. Typically, when an employee purposely destroys data or sends IP to a competitor or new employer, it usually results in a "my word against theirs" scenario. In this case, Tripp's actions in leaking confidential information are not in dispute, but his motive in doing so will significantly influence which party gets the protection of the court and the sympathy of the public. It all centers on the potential financial impact to a company; the context behind a breach becomes significantly more relevant once headline-grabbing regulatory fines, such as those from the General Data Protection Regulation (GDPR), are taken into consideration.

In *Int'l Airport Centers, L.L.C. v. Citrin*, an employee was sued for erasing data on his company laptop after deciding to go into business for himself.[30] And in October 2017, Todd Reyling was found guilty of copying and then deleting several of his employers' computer files before quitting his job.[31] Courts have held that even if an employee has access to files, that access is "no longer authorized" if they use the information in a way that is disloyal to their employer.[32]

In the case of a breach, a win in the courtroom by the employer proving negligence or bad intent by the employee is merely a Pyrrhic victory. Instead, it serves to highlight publicly an organization's deficient cybersecurity measures. Whether a judge rules in favor of an employer or an employee, executives will realize that the burden of proof in demonstrating adequate and appropriate technical and organizational security measures lies with their internal processes and systems. Organizations must identify malicious activity as it occurs and stop it before it harms critical systems and IP, and should take steps to inject workplace monitoring cybersecurity technologies into their IT environment to understand the full picture around an incident and prove end-user intent.

This is not to say that 2019 will be the year of “Us vs. Them,” or pit employee against employer. Employees have a vested interest in company success, and workplace monitoring is all about protection of people and data. Managing threats inside an organization through workplace monitoring is a vital element in a security professional’s toolbox—a reliable way to protect the company's customers, IP, and brand, as well as the good reputation of its employees.

However, workplace monitoring programs must be introduced with three key principles at their core: legitimate purpose, proportionality, and complete transparency during rollout. Protection of personal data and privacy are no longer best practices, but are basic essentials to any successful organization.

***We are awaiting legislation here in the United States that will be similar to GDPR. As an IT professional in healthcare, I believe data security and the protection of our patients as well as our employees is critical.***[34]

— Cody Taggart, System Administrator, Medical Arts Hospital

05

# A collision course to cyber cold war

## Trade embargoes prompt a surge of industrial espionage

***Prediction:***

*Isolationist trade policies will incentivize nation states and corporate entities to steal trade secrets and use cyber tactics to disrupt government, critical infrastructure, and vital industries.*

**Contributor:**
**Luke Somerville**
*Head of Special Investigations*

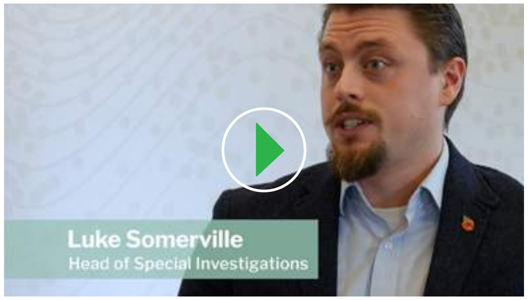
News outlets have described 2018 as the beginning of a 20-year trade war.[35] Historically, open trade borders have led to a cross-pollination of technology through existing and emerging markets. However, throughout 2018 we have seen a shift towards more protectionist postures in the form of trade embargoes—a result of fracturing trust between world powers.

On both sides, tariffs now accompany everything from consumer electronics to health and safety products. From the standpoint of disadvantaged nation-state players, trade disputes limit legitimate opportunities for the acquisition of software and hardware that could bolster their cyber capabilities. From an enterprise perspective, trade embargoes affect access to new technology, knowledge sharing, and even access to workforce talent.

Much commentary has been written around “cyber war” and its place alongside more conventional military techniques. This tends to result in fears of all-out war on the internet, and conjures visions of cyber attacks escalating into kinetic warfare. The Forcepoint 2017 Cybersecurity Predictions Report spoke of the implications of NATO Article 5, the new "Enhanced NATO Policy on Cyber Defense," which allows for kinetic war in response to an incident in cyberspace.[36] A better analogy for describing the likely implications of trade embargoes would be cold warfare, with cyber "operations" tied to the function of national foreign intelligence services. Changes to the flow and availability of information across national boundaries could lead to a future increasingly reminiscent of the years between the late 1940s and early 1990s, wherein access to technologies was acquired via espionage. Companies and nations have always been naturally protective of their IP, but as opportunities for legitimate access dwindle, people on the other side of embargoes will have real incentive to acquire it by nefarious means.

Instead of bigger walls to keep nation-state–sponsored hackers out of power generators and manufacturing plants, the cybersecurity industry needs to better understand how, when, and why people interact with this sensitive data, no matter where it is located. Nation states and enterprises alike need to understand who is touching critical content and why. To prevent IP theft, organizations should focus on understanding the normal behavior of legitimate users with access to trade secrets and knowing when this behavior changes—signaling an attempt to steal them. ■

**88%** of surveyed Forcepoint customers are concerned about potential attacks on the critical infrastructure their organization relies on.[37]



*Click above to see Luke Somerville, Head of Special Investigations, discuss this prediction.*

06

# Driven to the edge

## Organizations seek to bolster privacy, but make little headway due to broken trust

***Prediction:***
*Consumer concern about breaches will cause companies to embrace edge computing in order to enhance privacy. Designers will face significant headwinds with adoption due to low user trust.*

**Contributor:**
**Dr. Richard Ford**
*Chief Scientist*

For the average user, it feels like the news is filled with story after story of breaches or abuse of personal data. This constant stream of bad news has left many feeling as if no matter what they do, their information will eventually be spilled, only to resurface on the Dark Web some time later. Confidence in many online services is therefore running low, with optimism in short supply.

In response to these concerns, providers are attempting to balance the legitimate needs of user privacy with their own desire to monetize the services they provide. Even better, some developers have realized that, with sufficient effort, it is possible to apply the principles of “Privacy by Design” to create a solution that is mutually beneficial to both the service provider and the end-user.

One strategy for improving privacy is to allow customers to retain control of their data by moving the algorithms that help process it to the endpoint rather than sending the data to the cloud. This approach of leveraging the endpoint in harmony with the cloud is known as edge computing. While some people tend to view edge computing as in conflict with adoption of the cloud, it more accurately represents the full realization of the cloud computing vision—where the cloud and the endpoint work together to provide service.

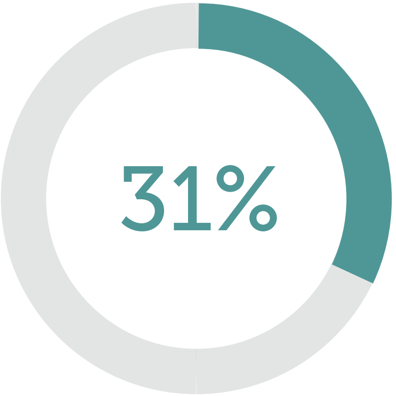
A recent example of a privacy-preserving solution that leverages edge computing is Apple's user trust scoring, which is designed to detect fraudulent use of a device by examining user behavior. As implemented, calculations on data are carried out on the device, with only metadata sent to the cloud, thereby protecting user privacy. However, these privacy benefits are only meaningful when end users are prepared to take the company at face value and actually believe that their data is, in fact, never moved off the device.

The drag here is trust. Because of the major shifts in societal trust over the last 10 years, trust in institutions has been replaced with a more distributed peer-to-peer (P2P) trust model. This is in part what has driven the success of companies like Uber and Airbnb, which essentially broker trust between two parties. No such process exists yet for companies, something that acts to the detriment of these better solutions. The emergence of security trust ratings may change the game. In so many ways, perception is reality.

Our prediction, then, is two-fold. First, we predict that many vendors will begin to apply the principles of edge computing in order to provide services with a higher degree of privacy. However, we also predict that many end users will either fail to understand these improvements, or have insufficient trust in the company to adopt these enhancements, thereby not allowing for real privacy to become a solid competitive differentiator.

It is not enough for organizations to comprehend and secure data both at the device and in the cloud. In order to engender trust they must make consumers believe that the company is indeed doing this. ■

*Click above to see Dr. Richard Ford, Chief Scientist, discuss this prediction.*



*Almost a third (31%) of Forcepoint customers surveyed are already limiting the data they place on the cloud due to security concerns.*[39]

07

# Cybersecurity cultures that do not adapt will fail

## Future “security trust ratings” reward some organizations, punish others

***Prediction:***
*Industry-wide “security trust ratings” will emerge as organizations seek assurances that partners and supply chains are trusted partners.*

**Contributor:**
**Meerah Rajavel**
*Chief Information Officer*

When an organization purchases services or signs a partnership deal, it undertakes significant due diligence based on financial security requirements and compliance with laws and industry standards. Today, our cloud-first, mobile-driven world sees users and data roam freely on networks, leaving critical data and intellectual property more exposed than ever. In the future, due diligence will extend to how much trust any organization can put into the security of a partner.

As such, 2019 will see the creation of industry-wide “security trust ratings.” Just as there are rankings and ratings for the trustworthiness of various financial institutions, investment options, or even restaurants, the future will bring a similar security trust rating to businesses that handle, store, or interact with data. These ratings would indicate how safe it is to permit suppliers to handle PII or other critical data. How does their employee cyber hygiene stand up? Does the supplier have a history or risk of breaches?

Forward-thinking companies should plan ahead, as their own security hygiene will now be as visible as industry accreditations or certifications.[40] There will be no way to hide from poor security habits and culture. As demonstrated by malware found in legacy systems at Micros, a division of Oracle and one of the top point-of-sale (PoS) suppliers globally, headline-grabbing hacks of supply chains not only have an immediate financial impact in the form of regulatory fines, but also damage company reputation and drive away future business.[41,42]

The way to develop an improved trust rating is through change in cybersecurity culture. Security cannot just be the responsibility of the IT teams and the technologies they implement, but must become a cultural and business value that is recognized and rewarded. To build a workforce united as a defense against cybercrime, organizations must integrate security into their culture from the top down.

Culture includes much more than the climate of a specific office location or the organization's values, norms, and rules. It also includes the chain of command, delegation of authority, accountability for behaviors, and broad communication strategies. Policies that are ill-defined or in conflict with one another create confusion and misinterpretation. Any confusion regarding rules, expectations, or accountability can increase risk—including risk of a data breach.

Today's corporate cultures have expansive boundaries that extend to supply chains and other partnerships due to connectivity and use of the cloud. As large organizations change their attitudes toward cybersecurity, this will be reflected throughout the supply chain. The introduction of security trust ratings will reward companies that move beyond superficial interventions—such as "just-in-time" training—which are ineffective and can result in employee annoyance, fatigue, and apathy.

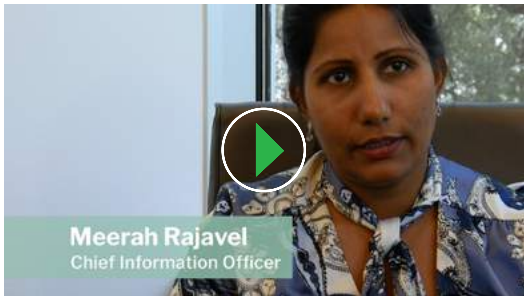
Companies that adapt their culture of security to sophisticated threats will win. However, they require systemic cybersecurity consistency across their operations and users, including their supply chain partners. ■

***Human mistakes are the biggest challenge and will always be a major issue.***[43]

— Business Professional, Large Enterprise Computer Services Company

***We're concerned about evolving malware and email threats, as well as new social engineering attacks. Because our employees may be our weakest link and we need strong security to be the safety net.***[44]

— IT Professional, Medium Enterprise Retail Company



*Click above to see Meerah Rajavel, Chief Information Officer discuss this prediction.*

*“Inconsistency is the biggest threat to an organization. There are always groups inside a company that think what they do is too important, or too different, and will push for an exception. In 2019, leaders need to help their teams understand that exceptions create significant risk for the broader organization.”*

**Jeff Brown**

*Vice President and CISO, Raytheon*

# Conclusion

In order to examine what will happen in 2019, we needed to look at the *why*, in order to help us predict the *what*. The motivation behind cyber actions, advanced malware development, or macro industry trends is essential to give us the context needed for accurate predictions. Enterprises can apply that approach when examining how best to protect their businesses, including their people and critical data.

Why is an end-user's communication not encrypted? Why is an attacker focusing their efforts on targeting a specific industry? Why did that obvious malicious behavior go undetected?

Cybersecurity professionals know that specific attacks will change and evolve, but the themes remain the same: sensitive data is an attractive target for attackers. Threat actors, malware authors, the "bad guys"—call them what you will—keep inventing new methods to bypass protection systems devised by the cybersecurity industry. Attackers and security analysts expend efforts in a continuous cycle of breach, react, and circumvent—a true game of cat-and-mouse.

We need to escape this game; by taking a step back every year to examine trends and motivations, we're able to see the overall forest among the millions of trees.

The concept of trust is embedded throughout our seven predictions for 2019. Trust is vital to personal and business relationships. It can make or break a business, yet it is intangible. Consider trust to exist on a continuum between complete faith and absolute mistrust; in the middle of that continuum, there is a grey area of uncertainty.

The option to "trust but verify" might be applicable in some scenarios, but only if supported by visibility into the cyber behavior of an end-user. It's a challenge to make a security decision if the risk barometer does not swing clearly one way or the other. The risk may be transferred because control was delegated throughout the supply chain, perhaps to a cloud provider who now manages the location of the data and even the authentication of users to limit access to the data.

***The way to gain control is through behavioral modeling of users or, more specifically, their digital identities. Understanding how a user acts on the network and within applications can identify anomalies, bring about understanding of intent, and gain trust. Behavior might be deemed low risk or high risk, or undetermined. Deeper understanding of behavior means we can be stronger in our determination of trust and risk. Instead of making a black-and-white decision like traditional security approaches, the cybersecurity response now and in the future can adapt as risk changes, without introducing business friction, allowing us to stop the bad and free the good.***

As always, we will review the accuracy of our 2019 cybersecurity predictions throughout the year. After all, you trust us to get them right. ■

## Works cited

1. Kuranda, Sarah. “Study: Cybersecurity Skills Gap Will Grow To 3.5M Positons By 2021.” *CRN*, 6 June 2017, www.crn.com/news/security/300086546/study-cybersecurity-skills-gap-will-grow-to-3-5m-positons-by-2021.htm.
2. McCormick, J. *Predictions 2017: Artificial Intelligence Will Drive The Insights Revolution*. Forrester, 2 Nov. 2016.
3. *Automotive Artificial Intelligence Revenue to Reach $14 Billion by 2025, According to Tractica | Business Wire*. 24 May 2017, https://www.businesswire.com/news/home/20170524005456/en/Automotive-Artificial-Intelligence-Revenue-Reach-14-Billion.
4. Solon, O. *The Rise of 'pseudo-AI': How Tech Firms Quietly Use Humans to Do bots' Work | Technology | The Guardian*. 6 July 2018, https://www.theguardian.com/technology/2018/jul/06/artificial-intelligence-ai-humans-bots-tech-companies.
5. Hornigold, T. *How Fast Is AI Progressing? Stanford's New Report Card for Artificial Intelligence*. 12 Jan. 2018, https://singularityhub.com/2018/01/18/how-fast-is-ai-progressing-stanfords-new-report-card-for-artificial-intelligence/#sm.00001vlq30ylzcs1sf722zbsynfyj.
6. Shoham, Y., R. Perrault, E. Brynjolfsson, and J. Clark. *Artificial Intelligence Index 2017 Annual Report*. Nov. 2017, https://aiindex.org/2017-report.pdf.
7. *AI: 15 Key Moments in the Story of Artificial Intelligence*. https://www.bbc.com/timelines/zq376fr.
8. Dvorsky, George. Hackers Have Already Started to Weaponize Artificial Intelligence. Gizmodo, 12 Sept. 2017, gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425.
9. Lorica, B., and P. Nathan. 5 Findings from O'Reilly's Machine Learning Adoption Survey Companies Should Know - O'Reilly Media. 7 Aug. 2018, https://www.oreilly.com/ideas/5-findings-from-oreilly-machine-learning-adoption-survey-companies-should-know.
10. Source: TechValidate. TVID: 108-7E9-1A6
11. “2018 Security Predictions, by Forcepoint Security Labs.” *Forcepoint*, 21 June 2018, www.forcepoint.com/resources/reports/2018-security-predictions-forcepoint-security-labs.
12. Melendez, Steven. “Spectre” And “Meltdown” Chip Flaws Touch “Almost Every System,” Say Researchers. Fast Company, 4 Jan. 2018, www.fastcompany.com/40513416/spectre-and-meltdown-chip-flaws-touch-almost-every-system-say-researchers.
13. Source: TechValidate. TVID: CBE-B96-18C
14. Source: TechValidate. TVID: 680-5DE-BF9

15. Source: TechValidate. TVID: 6B7-B75-241

16. Thomas, Kurt, et al. Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials – Google AI. Google AI, 1 Jan. 1970, ai.google/research/pubs/pub46437.

17. Krebs, Brian. Hanging Up on Mobile in the Name of Security. Krebs on Security, 16 Aug. 2018, https://krebsonsecurity.com/2018/08/hanging-up-on-mobile-in-the-name-of-security/.

18. Waddell, Kaveh. Fake Fingerprints from an Inkjet Printer Can Fool Your Smartphone. Atlantic Media Company, 8 Mar. 2016, www.theatlantic.com/technology/archive/2016/03/fake-fingerprints-from-an-inkjet-printer-can-fool-your-smartphone/472638/.

19. Schlesinger, Jennifer. Why the Emerging Ransomware Threat's next Target Could Be Your Smartphone or Tablet. CNBC, 20 May 2017, www.cnbc.com/2017/05/19/new-hacking-threats-fingerprint-vulnerabilities-and-sophisticated-ransomware.html.

20. Peterson, Becky. Apple Worked with Hollywood Mask Makers to Make Sure the IPhone X's Facial-Recognition System Can't Be Fooled Easily. Business Insider, 12 Sept. 2017, www.businessinsider.com/apple-says-the-iphone-xs-face-id-system-cant-be-fooled-by-masks-2017-9.

21. Newman, Lily Hay. Hackers Trick Facial-Recognition Logins With Photos From Facebook (What Else?). Conde Nast, 19 Aug. 2016, www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/.

22. Koong, et al. A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices. The Scientific World Journal, 24 July 2014, www.hindawi.com/journals/tswj/2014/781234/.

23. "IBM Security Risk Based Authentication Solution." IBM Security Risk Based Authentication Solution - Overview - United States, IBM, 23 Oct. 2018, www.ibm.com/us-en/marketplace/risk-based-authentication-solution?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US.

24. Source: TechValidate. TVID: 113-FE0-D0C

25. Bantz, Phillip. "One CLO Tested His Employees' GDPR Knowledge and Was 'Shocked' at What He Found." Legaltech News, 2 Aug. 2018, www.law.com/legaltechnews/2018/08/02/one-clo-tested-his-employees-gdpr-knowledge-he-was-shocked-at-what-he-found-397-10326/?slreturn=20180923031020.

26. 24% Of UK Employees Maliciously Misuse Company Emails: Research. CISO MAG, 7 Nov. 2017, www.cisomag.com/24-uk-employees-maliciously-misuse-company-emails-research/.

27. "Privacy Regulator Warns MPs over Shared Passwords." BBC News, BBC, 4 Dec. 2017, www.bbc.com/news/technology-42225214.

28. Sher-Jan, Mahmood. Data Indicates Human Error Prevailing Cause of Breaches, Incidents. The Privacy Advisor | Data Indicates Human Error Prevailing Cause of Breaches, Incidents Related Reading: IAF, Hong Kong DPA Release Ethical Accountability Report, Framework, 26 June 2018, iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/.

29. Isidore, Chris. Tesla Sues Ex-Employee for Hacking and Theft. But He Says He's a Whistleblower. CNN, 20 June 2018, money.cnn.com/2018/06/20/technology/tesla-sues-employee/index.html.

30. FindLaw's United States Seventh Circuit Case and Opinions. Findlaw, www.caselaw.findlaw.com/us-7th-circuit/1392048.html.

31. United States District Court, S.D. Illinois. KASKASKIA ENGINEERING GROUP, Plaintiff, v. TODD REYLING, Et Al., Defendants. 2 Oct. 2017.

32. 18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computers. Cornell Law School, www.law.cornell.edu/uscode/text/18/1030.

33. Source: TechValidate. TVID: A0A-01D-862

34. Source: TechValidate. TVID: 541-863-071

35. Hankla, Charles. The next Cold War? US-China Trade War Risks Something Worse. The Conversation, 24 Sept. 2018, theconversation.com/the-next-cold-war-us-china-trade-war-risks-something-worse-103733.

36. "The 2017 Forcepoint Security Predictions Report." *Forcepoint*, 13 Aug. 2018, https://www.forcepoint.com/resources/reports/2017-forcepoint-security-predictions-report.

37. Source: TechValidate. TVID: 900-9BB-779

38. Cuthbertson, Anthony. Apple Is Quietly Giving People Black Mirror-Style 'Trust Scores' Using Their iPhone Data. Independent Digital News and Media, 21 Sept. 2018, www.independent.co.uk/life-style/gadgets-and-tech/news/apple-trust-score-iphone-data-black-mirror-email-phone-fraud-a8546051.html.

39. Source: TechValidate. TVID: 214-C6D-148

40. All Clouds Are Not Equal - Forcepoint Cloud Compliance. Forcepoint, 7 Mar. 2018, https://www.forcepoint.com/all-clouds-are-not-equal-forcepoint-cloud-compliance.

41. Ashford, W. O*racle Micros Breach Highlights PoS and Supply Chain Security Risks*. 21 June 2016, https://www.computerweekly.com/news/450302206/Oracle-Micros-breach-highlights-PoS-and-supply-chain-security-risks.

42. Drinkwater, Doug. "Does a Data Breach Really Affect Your Firm's Reputation?" CSO Online, CSO, 7 Jan. 2016, www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html.

43. Source: TechValidate. TVID: 214-C6D-148

44. Source: TechValidate. TVID: B30-66D-75E

45. Source: TechValidate. TVID: C4A-4A6-FA4

Want to learn more about the 2019 Predictions?

watch the webcast ›

**About Forcepoint**

Forcepoint is the global human-centric cybersecurity company transforming the digital enterprise by continuously adapting security response to the dynamic risk posed by individual users and machines. The Forcepoint Human Point system delivers Risk-Adaptive Protection to continuously ensure trusted use of data and systems. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries. **www.forcepoint.com** [500006.111218]