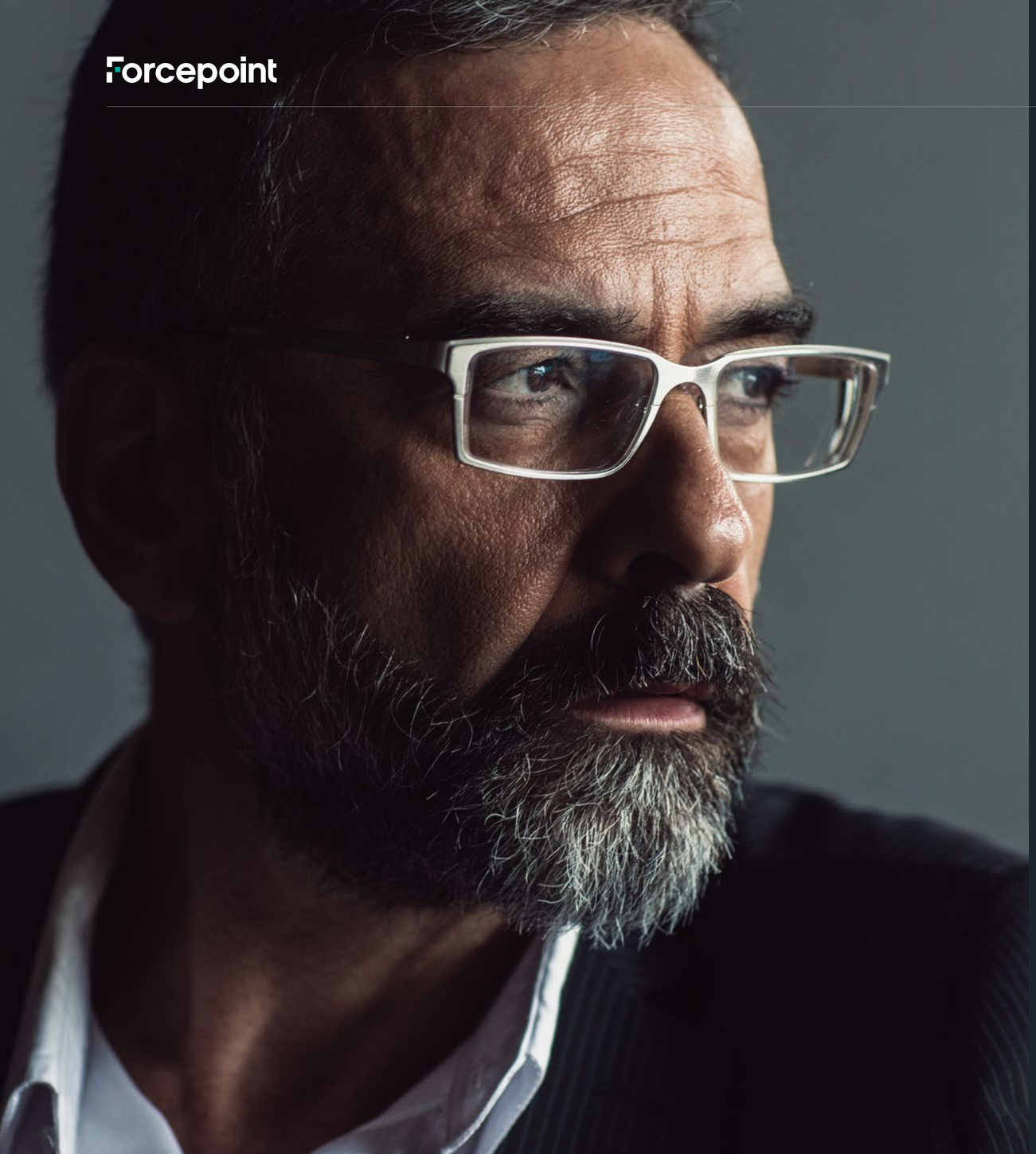

Forcepoint

Ebook

Future Insights 2021

forcepoint.com

Forcepoint
Future Insights 2021

Every year, Forcepoint cybersecurity experts from across the business come together to assess how the industry has changed in the last 12 months, and what is likely to happen in the next year. Forcepoint Future Insights offers six separate points of view from individual contributors on the trends, and events we believe the cybersecurity industry will need to deal with in 2021. This analysis, driven by Forcepoint X-Labs, ignites interesting conversations and we look forward to debating them in the next few months.

And then suddenly...

Chaotic and unpredictable are the words that describe 2020 most accurately. In February, work and life went on as usual, with the typical struggles with technology and security. And then came March. As workers moved from onsite to remote, IT, security and corporate leadership was forced to accelerate their digital transformation, and, as we all became more reliant on technology across work, school, and entertainment, cybersecurity threats increased exponentially.

Adaptability is another key term and lesson from 2020. COVID-19 required CISOs to take a hard look at what worked and what needed improvement. Human behavior played a huge role in the effectiveness of cybersecurity in a work-from-home model, and Forcepoint experts foresee a human-centric security approach as the way forward in this evolving digital environment.

But to look forward, we have to understand what 2020 taught us. What did we learn from those hundreds of Zoom meetings and the need to upgrade security across cloud applications? As artificial intelligence and machine learning play a bigger role in behavior analytics, is it time to address the bias built into the technology? And how well did we do at protecting our data while working remotely? Forcepoint experts offer their insights on these questions and more, offering a blueprint for cybersecurity approaches in 2021 and beyond.

The Emergence of the Zoom of Cybersecurity

I always love looking toward the future, but in 2020 it seems that the future rushed right at us, startling us and shaking us all up. Now we've had a little time to adapt, we can regroup, reassess and take steps forward again.

This is the status quo today we have all moved to remote working. Cloud deployment is a necessity. Digital transformation has happened; and where it hasn't, it needs to.

All of these macro factors has led me to conclude that cybersecurity is now a business differentiator, and it needs a category disruptor. Cybersecurity has become the enabling engine that permits businesses to accelerate their pivot to the cloud and take advantage of the speed, scale and resilience of digital transformation.

The understanding and position of cybersecurity within the boardroom has long been an area for debate. Now, our discipline has moved a step higher in the foodchain, and our importance is elevated. What will happen in 2021 to the industry?

The Irresistible Force

When Gartner first introduced SASE as a concept in 2019, their first report indicated that the market would not be ready or would not move to this model for between three and five years. Only 40 percent of companies will move to the model by 2024. But a combination of existing market forces in shifting to the cloud, plus the new blueprint of remote working forced upon us, means we're facing a faster defragmentation of the market and an emergence of the "security platform" as the tool of choice.

This puts us in a situation rather like the irresistible force paradox. When an immovable object, in this case, the way cybersecurity is perceived at board level, meets an unstoppable force, here digital transformation driven by both market change and the events of 2020, what happens? It's my view that in fact the immovable object moves. Cybersecurity grows in importance at the board level, thus driving demand for security cloud platforms. Boards of directors seek out differentiation and innovation for their businesses, speedy solutions and cost savings: all of which will deliver pressure for security in the cloud, and thus a need for a cloud platform security solution.

These changing demands at the top will deliver metamorphosis within the cybersecurity industry. The need for a converged, digital, cloud-delivered platform means we'll see **the emergence of the "Zoom of Security."** As we all discovered this year, Zoom "just works." It's a high-tech system that is easily accessible for the everyday consumer, and this is what boards will demand of their cybersecurity platforms.

Any serious category disruptor must be more deeply integrated into the public cloud ecosystem. Currently, developers are using security as a tool, but having to shoehorn in applications and functions not necessarily designed as cloud-native. Security will move to the left for the developer, and will become easily deployable and fully integrated.

> Security will become so ingrained in applications and platforms that people will no longer realize they are being "secured."

NICO POPP
CHIEF PRODUCT OFFICER

Security... by Stealth?

This integration will result in security becoming so ingrained in applications and platforms that people will no longer realize they are being "secured." Cybersecurity products have long been tarred with the brush of being intrusive, conflicting with people's ability to get the job done, thus constricting innovation. Even for cybersecurity practitioners, the security stack is too complex. It's got to become more automated, delivering security as a service so that enterprises can get on with their core business: not their core business plus running a team of expert cybersecurity professionals.

Analysts agree: in fact Forrester is predicting that Zero Trust architectures will grow 200% in 2021. Once we emerge out the other side of this shift, security will be a cloud commodity, and the combination of technology plus data will give IT leaders true visibility of how and where data is moving through an organization.

It is this visibility of data which is the game changer. It's not about monitoring in terms of keeping tabs on people's actions, or invading their privacy: it's about giving data analysts and business leaders a clear line of sight over data and its movements. Behavioral analytics gives us the telemetry we need to make intelligent, risk-based decisions on the fly, without intruding on either people's privacy or their workflows.

We will have some fun to look forward to next year. In my view, this category disruptor is likely to emerge through vendor consolidation or market movements, so we should also expect some significant merger and acquisition activity within the cybersecurity sector in 2021.

This defragmentation of the market, and shift to cloud and converged platforms alongside vendor consolidation, should mean that security gets easier for business leaders—and hopefully for the professionals on the frontline too. Cloud will become part of cybersecurity's DNA in a way that it isn't today.

Finally Taking Action Against Inherent Bias in Machine Learning

Cracks in Trust and How to Mend Them

Looking at the cybersecurity landscape today, I have to say I'm glad I'm not a CISO. In an ever-evolving world of digital transformation, omni-connected devices and semi-permanent remote workforces, keeping critical data and people safe is a huge challenge. So huge, in fact, that it can't be done without implementing machine learning and automation.

At the core of understanding risk and exposure to an organization, we need to understand its critical data and how that data moves. We can only do so by collecting large quantities of metadata and telemetry about said data and the interactions with it. We can then apply analytics to make sense of the data and translate it into a risk-based view.

However, developing automated systems is not without its challenges, and in 2021 I believe that machine learning and analytics will fall under tighter scrutiny, as trust in their unbiased nature and fairness as well as ethical boundaries will be questioned.

Rage at the Machine

We saw headline-grabbing incidents this summer. For example in the United Kingdom, where the government initially decided to let algorithms determine schoolchildren's exam results. However, the bias that had been baked into this algorithm resulted in significant drops in grades, unfairly skewed to lower-income areas, and worse, not taking the teachers' expertise into account. This resulted in an embarrassing U-turn, where people ended up trumping machines in grading exams.

This is not the first time that algorithms and machine learning systems trained on biased data sets have been criticized. You will have heard of Microsoft's Tay chatbot and you may have heard of facial recognition software incorrectly identifying members of the public as criminals. Getting it wrong can have life-changing effects (e.g. for the students or people applying for credit) or could be as "minor" as an inappropriate shopping coupon being sent to a customer.

A number of cybersecurity systems use machine learning to make decisions about whether an action is appropriate (of low risk) for a given user or system. These machine learning systems must be trained on large enough quantities of data and they have to be carefully assessed for bias and accuracy. Get it wrong, apply the controls wrong, and you will experience situations such as a business-critical document being incorrectly stopped mid-transit, a sales leader unable to share proposals with a prospect or other blocks to effective and efficient work. Conversely if the controls are too loose, data can leak out of an organization, causing damaging and costly data breaches.

Machine learning systems must be trained on large enough quantities of data and they have to be carefully assessed for bias and accuracy.

RAFFAEL MARTY
VICE PRESIDENT OF RESEARCH AND INTELLIGENCE, X-LABS

Finding the Balance in 2021

To build cyber systems that help identify risky users and prevent damaging actions, the data we analyze comes for the most part from looking at a user's activities. It's worth saying upfront that user activity monitoring must be done appropriately, and with people's privacy and the appropriate ethical guidelines in place.

In order to create a virtual picture of users, we can track log-on and log-off actions. We monitor which files people open, modify and share. Data is pulled from security systems such as web proxies, network firewalls, endpoint protection and data leak prevention solutions. From this data, risk scores are then computed and the security system in turn flags inappropriate behaviour and enforces security policies appropriately.

When undertaking this analysis or, in fact, any analysis which uses machine learning or algorithms to make automated decisions that impact people's lives, we must use a combination of algorithms **and human intelligence**. Without bringing in human intuition, insights, context and an understanding of psychology, you risk creating algorithms that are themselves biased or make decisions based on flawed or biased data, as discussed above.

In addition to involving human expertise in the algorithms, or in other words, modelling expert knowledge, the right training data and the right data feeding the live analytics are just as important. What constitutes the "right" data? Or, in a similar question, how long is a piece of string? The right data is often determined by the problem itself, how the algorithm is constructed and whether there are reinforcement loops or even explicit expert involvement is possible. The right data means the right amount, the right training set, the right sampling locations, the right trust in the data, the right timeliness, etc. The biggest problem with the 'right data' is that it's almost impossible to define what bias could be present until a false result is observed and it's potentially too late; harm has been caused.

Using machine learning and algorithms in everyday life is still in its infancy but we see the number of applications grow at stunning pace. In 2021, I expect further applications to fail due to inherent bias, and a lack of expert oversight and control of the algorithms. Not the least problem being that the majority of supervised machine learning algorithms act as a blackbox, making verification either impossible or incredibly hard.

This doesn't mean that all machine learning algorithms are doomed to failure. The good news is that bias is now being discussed and considered in open groups, alongside the efficacy of algorithms. I hope we will continue to develop explainable algorithms that model expert input. The future of machine learning is bright; the application of algorithms in smart ways is only bounded by our imagination.

Additional Resources

For more detail on Forcepoint's commitment to privacy, please see the Forcepoint Privacy Hub.

People Do People Things: The Future of Security is Human

As 2020 comes to an end, the importance of understanding the relationship between humans and technology is at an all-time high. Widespread shifts in the fabric of our society, prompted by the ongoing pandemic, exposed weaknesses in security tools and protocols for remote workers, highlighted issues of network reliability and accessibility and demanded that humans find innovative ways to keep organizations running. While the fallout from the pandemic is unquestionable, the ability for people to respond to seemingly endless challenges has been nothing short of remarkable.

The year 2021 will continue to reflect human resilience and ingenuity. It will be the year of workarounds and self-serving insider threats, where people find ways to accomplish their goals despite dealing with personal and professional adversity. Workarounds, shortcuts and creative work strategies are simultaneously a celebration of human creativity and a risk for organizations that are desperately trying to maintain visibility of their assets. Ultimately, people sharing data and accessing corporate networks in new and potentially unsanctioned ways carries quite a bit of risk—especially for organizations that are new to managing remote workers.

The result of these changes is that successful cybersecurity strategies will stop trying to use technology as a unilateral force to control human behavior. Rather, organizations will come to terms with the reality that adding more and more technology or security does not lead to behavioral conformity, especially not conformity that aligns with security principles and adequate cyber hygiene. In fact, additional layers of security may push more people outside of the guide rails due to increasingly aggravating security friction that blocks them from completing tasks or easily accessing critical organizational assets.

Understanding Precedes Predicting

Understanding how people adapt to, respond to, and inform their environments is critical for organizations heading into the new year. For far too long, the tech world has created products with the assumption that people will use them in an expected or uniform way, or that people would conform to the rules and constraints laid out by well-meaning engineering teams. If we've learned anything from 2020, it is that people are not always predictable, and making assumptions about human behavior is a dangerous game to play. What's surfaced is that expectations, guidelines, best practices and even commands will yield every type of behavioral response—from rigid compliance to retaliatory noncompliance.

What can we do? We can learn more about what motivates behavior, and how people ultimately choose to behave. We can also commit to designing and implementing security practices and tools that work *with* humans instead of against them. To do this, however, we have to focus on measuring and understanding behavior instead of focusing exclusively on detecting compromises and vulnerabilities.

For instance, we know that people's immediate needs often outweigh potential negative consequences—especially when the consequences do not have a direct, individual, and immediate impact. This means that when we need to accomplish our goals we often take the easiest route. Unfortunately, the easiest route is often riskier than the "ideal" route. When faced with frustrating, security-heavy file and data sharing tools, we may turn to sharing via personal cloud applications. Making rules to stop people from engaging in this type of behavior is not working—so rather, we have to better understand these behaviors to find ways to mitigate their risk to organizations and organizational assets.

> Successful cybersecurity strategies will stop trying to use technology as a unilateral force to control human behavior. More and more technology and security does not lead to behavioral conformity.

DR MARGARET CUNNINGHAM
PRINCIPAL RESEARCH SCIENTIST

Building Behavioral Understanding Into Systems

Within the cybersecurity industry, observing and understanding behaviors must come with context. What may appear at first glance like an obviously malicious act likely to lead to data loss—for example an engineer requesting access to multiple sensitive data repositories over the course of two days—could simply be a person getting their job done. Our engineer may be doing this because she's been added to several new projects and needs to be able to collaborate with her new team.

We want people to be able to do their jobs within the constraints of our corporate network and policies, so blocking them would only encourage the human tendency to find an easier (and less secure!) route for getting their jobs done. With an interdisciplinary research team, pulling experts from security, counter-intelligence, IT and behavioral sciences together, behavioral understanding can be built into cybersecurity systems. And this is the first important step for finally starting to move cybersecurity left of breach—designing security for the human element.

In 2021 and Beyond, Disinformation is Inevitable

In 2021 and beyond, disinformation is inevitable as people continue to believe what they read at face value without any additional research. Most Americans are now aware of the fact that Russians, through hacks and disinformation, attempted to influence the 2016 election. Admiral Mike Rogers, who ran the National Security Agency, says that, in hindsight, not enough was done to combat disinformation. "I don't think we really fully understood the magnitude," he told *All Things Considered*.

Since then, there have been countless instances of high-profile disinformation campaigns and attacks. In 2018, the Cambridge Analytica scandal came to light; Facebook user data was covertly harvested by the British political consulting firm. More recently, a *Guardian* headline declared: "Facebook is out of control. If it were a country it would be North Korea." In a related story, much has been said about the Brexit disinformation scheme considered the "greatest electoral fraud perpetrated in Britain for more than a century." Fake explosion videos, election meddling efforts, contrived protests, and more—it seems the Internet Research Agency may be the best at sowing discord, confusion, and disinformation that others will continue to follow—and believe.

> Public/private partnerships could help combat disinformation campaigns and bad actors.
>
> **ERIC TREXLER**
> VP OF SALES, GLOBAL GOVERNMENTS

Currently, disinformation is one of the biggest yet most nebulous threats facing democracy. It's a high-stakes, low-consequence information war. Adversaries are turning technology and our core values against us. How do you combat the abuse of the First Amendment without trashing the spirit of the First Amendment? The Internet was founded on anonymity, which makes disinformation difficult to combat. It's cheap, it's easy and people want to believe what they read when it aligns with their ideas and mindset. At the same time, it's gotten easier to create deepfakes and malicious bots, as the tools behind them have been democratized and widely disseminated. We've even seen the rise of disinformation-as-a-service which, when weaponized against corporations, can be "extremely painful, knock billions off share prices and cost CEOs their jobs," Sharb Farjami, global chief executive officer of Storyful, told the *Financial Times*.

However, the government has more recently turned its attention to big tech and the monopolies they have carved out for themselves in recent years. In fact, a majority of the public now supports regulation of big tech companies. Just as the FCC regulates television and radio in the United States, there is mounting pressure for governmental oversight of social media platforms to rein in the runaway disinformation issue. The Honest Ads Act, for one, would mandate the same transparency with regard to social media advertising that's required of traditional advertising, which is a step in the right direction.

Still, disinformation comes in multiple forms. There is simply no silver bullet to remedy the threat—no single tool that can guide people to truth or safety. Instead, everyone must be diligent about questioning what they see online, as opposed to simply taking information at face value without further thought or inquiry. The good news is that compared to several years ago, there's much more awareness today on disinformation campaigns and their intent, as well as growing dialogue with social media organizations around the issue.

Additionally, public/private partnerships could help combat disinformation campaigns and bad actors—particularly in the U.S. and U.K., where open standards can leave organizations more open to attack. The Carnegie Endowment recently suggested a consortium that brings together academics, large social platforms and commercial tech companies to ramp up disinformation research. Historically speaking, innovation is largely driven by necessity. While disinformation is a large and growing threat, it's exciting to think what new technology could come from such an initiative, or how social media could evolve to meet this urgent challenge.

In 2021 and beyond, disinformation will continue to increase in focus and scope. And why not? Disinformation campaigns are easy and low-cost to implement, while the risk and penalties are nearly non-existent.

The Rise of Insider Threat-as-a-Service

The Biggest Threats Will Come from the People And Places You Least Expect

When envisioning the threats to your organization, malicious nation states or greedy virtual thieves located halfway around the world might loom large. But what if the risk is an undercover employee? What if it's a person who's not even real? What if it's the neighbor you never suspected? In 2021 we're going to see threats emerge from unexpected places, and sometimes the call will be coming from inside the house.

Insider threat needs to be taken seriously and accepted as a real risk by security leaders, who must ask tough questions about whether they have the tools in place to spot and stop anomalous behavior.

MYRNA SOTO
CHIEF STRATEGY AND TRUST OFFICER

Insider Threat-as-a-Service

In the past we've thought of "insider threats" as disgruntled employees who walk out of the building with proprietary information hidden in their briefcases. But today, your employees may be scattered around the world, you may hire them after only meeting via Zoom, and they may never step foot inside one of your offices. And today, you can buy almost anything on the dark web, including "trusted insiders." In 2021, I expect to see organized cells of recruitment infiltrators offering specifically targeted means for bad actors to become trusted employees, with the goal of exfiltrating priceless IP. These "bad actors," literally, will become deep undercover agents who fly through the interview process and pass all the hurdles your HR and security teams have in place to stop them.

We want to believe our employees are good people—but the stats tell us that between 15 and 25 percent are not. The only way to find these people before they do irreparable damage to your organization is by understanding human behavior and knowing when their activities don't match their profile.

Synthetic Identities

I believe we'll see another form of fake identity -coming specifically for the financial services industry in 2021.

According to McKinsey, synthetic ID fraud is the fastest-growing type of financial crime in the United States and is spreading to other geographies. Synthetic fraudsters use real and fake credentials to build a phony profile good enough to apply for credit. Although the applications are normally rejected by the credit bureau, having a file is enough to set up accounts and start building a "real" credit history to apply for bank accounts, credit cards and loans. It's almost impossible to tell a real identity from a synth, and since there's no individual person whose ID is stolen, the real victims are the businesses left with no way to recover their losses.

You would think that modern technologies such as machine learning (ML) could easily identify this kind of fraud. The issue is finding the data set to train the ML: how do you show it how to identify a fake persona when they're almost indistinguishable from real people?

The answer is to dig deeper to establish identity with third party data feeds that show a consistent history or a face-to-face identification of a passport or driving license. Over time, businesses can build a checklist of inconsistencies commonly found in synthetic identities and use this to train an algorithm to automatically flag suspect files for action.

> We'll see the rise in another form of fake identity specifically damaging to the financial services industry—synthetic ID fraud.
>
> **MYRNA SOTO**
> CHIEF STRATEGY AND TRUST OFFICER

The Hacker Next Door

We know from our studies into behavior that it's easier, and more comfortable, for cybersecurity professionals to believe that all attacks come from external forces, and picture the attackers as devious foreign actors. But the truth is, nation states usually have higher value targets in sight than schools or hospitals. They also want to fly under the radar: when stealing a formula for a vaccine for example, it's more valuable if no one realizes it's missing.

Annoyance attacks or DDoS hits also often have local suspects. For example, who knows a school system's security better than a student who uses the network, and who has a better reason to cause a disruption?

Miami-Dade Schools found this out the hard way when a 16-year-old student was revealed as the mastermind behind a cyberattack on the first day of school. The network was overwhelmed with DDoS attacks causing error messages and glitches that disrupted virtual classrooms for days.

Very often when it's a data breach, it's more likely to be coming from the inside. We see many cases of low-level data theft from employees who think they won't get caught, and certainly a whole host of data breaches caused by simple human error or poor security administration. With COVID-19 continuing to push work and education to the home and hospitals increasingly utilizing telemedicine to treat patients, thousands of enterprises are more reliant on technology, and more at risk from troublesome insiders, than ever before.

Insider threat needs to be taken seriously and accepted as a real risk by security leaders, who should ask tough questions about whether they have the tools and solutions in place to spot and stop anomalous behavior, before it's too late.

Where is Your Data? You'll Find Out in 2021 (One Way or the Other)

As we near the end of 2020 I imagine there are many CISOs, CIOs and business leaders patting themselves on the back for successfully transitioning their workforce from the corporate office to remote or hybrid office-and-home systems. Employees have successfully adapted, happily and productively accessing data and continuing to work in a new way. It's true that IT and security teams have been, as so often the case, unsung heroes for making the impossible possible in the first half of the year. However I'm afraid I need to burst this bubble. In 2021 I believe we will start to realize exactly how much intellectual property was stolen by external attackers and malicious insiders in the shift to remote working in 2020. We will see the full impact of the remote working shift on work culture, infrastructure security and the protection of data everywhere.

To achieve this goal, we must introduce real-time user activity monitoring. Cloud-native solutions with a deep understanding of users' behavior will deliver permanent solutions, rather than stopgaps.

NICOLAS FISCHBACH
CHIEF TECHNOLOGY OFFICER

What Did We Do?

Almost overnight organizations flipped a switch from a predominantly office-based workforce to remote workers using a plethora of operating systems and equipment. Employees with a wide range of technical know-how were left to set up and configure home networks and devices, while IT teams added and tried to scale VPNs and moved data into SaaS applications. It is almost as if companies gave up on protecting the perimeter and trusted in basic networking and cloud services to protect what I call the "branch office of one." The old perimeter is clearly gone, data needs to be more accessible than ever, and the ability for the user to work remotely is paramount.

It's my view that we don't yet know what impact remote working has had, and 2021 will start to unveil it to us.

- → Did we keep an eye on our attack surface and did we really examine the vulnerabilities we exposed during this time?
- → When cloud service providers spun up new clouds or SaaS applications for us, did the security keep pace and did our policies get applied consistently?
- → Has lockdown meant that cyber-enforcement got lighter? Did cybercriminals think they could get away with stealing data while security and IT teams' attention was elsewhere?

The treasure trove has been opened right up, and security teams should not rest on their laurels. From past experience, I must assume that we haven't moved as fast as the attackers. In 2021, we will see several large data breaches revealed. Some firms will discover to their horror that their defenses have been infiltrated by what appears to be nation-state attackers or well-organized criminal groups.

Like it forcefully happened to digital transformation programs, the notion of multi-year security programs will be replaced, in 2021 and beyond, with more agile security. We need to move at the speed of the bad guys, and our responses to threats must be completed at the same rate of change we would expect from a business model pivot or adaptation.

> Companies gave up on protecting the perimeter, and trusted in basic networking and cloud services tp protect "the branch office of one".

NICOLAS FISCHBACH
CHIEF TECHNOLOGY OFFICER

The Imperative of Visibility in 2021

Data visibility and the management of data protection is the most important cybersecurity imperative for enterprises in the next year. In this way, 2021 can become the year of working securely, regardless of location. These new patterns are here to stay, and we must do our best to introduce resiliency, security and visibility into our efforts.

As part of this, we must address the elephant in the room. Data loss is damaging to business, and in order to stop that loss, we need to know exactly where our data is, on a minute-by-minute basis.

That means we must introduce real-time (or near real-time!) user activity monitoring. We should be monitoring to prevent data loss: not productivity tracking. Transparency in the roll-out of these solutions and the careful consideration of user privacy should be at the heart of any user activity monitoring solutions. Forrester analyst Dr. Chase Cunningham has advised: "If you aren't monitoring your data, your intellectual property is walking out of the door, and you'll be out of business in twenty years."

The fact that we have shifted to remote working so quickly, and relatively smoothly, may mean that we have no need to go back to a structured perimeter. But we will need to move quickly toward user activity monitoring—an approach that relies on analytics to understand data access patterns and indicators of Behavior (IoB) that can indicate levels of risk. Without visibility of data in this way we cannot scale and understand how to work productively, flexibly and securely. Through the combination of behavioral analytics and IoBs to form the foundation of dynamic risk assessment, we can achieve visibility. Data usage must be examined and understood in context, and data loss prevention policies applied adaptively, and dynamically. If we can create cybersecurity technologies which build upon machine learning and analytics to measure and understand data movements in quasi real-time, we can avoid the upcoming dawn of disappointment on the horizon.

As the "new normal" becomes "just normal", leaders must get the basics right: revisit their policies and processes, validate their posture and risk appetite, and avoid assumptions that all is well just because they haven't seen an incident yet. Longer term, cloud-native solutions with a deep understanding of users' behavior will deliver permanent solutions, rather than stopgaps when it comes to protecting data and intellectual property.

Forcepoint

Future Insights 2021

Stop the bad. Free the good.

What can we expect from 2021? If 2020 and the pandemic taught us anything, it is that we must be prepared to handle any challenge thrown our way. In our new normal, millions of employees will continue with full-time or a hybrid-model of remote work, and threat actors will have newer, more sophisticated techniques to infiltrate our networks and compromise our data.

As work cultures continue to evolve in 2021, business and security leaders will seek to keep their people and their data safe while freeing their employees to do their jobs from anywhere. Only by stopping the bad and freeing the good will enterprises be truly agile and operating securely without boundaries in the coming months and beyond.

→ **Watch Nico Fischbach and Myrna Soto as they discuss the Future Insights**

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[Forcepoint-Future-Insights-2021-Ebook-EN] 07Dec2020