2020 Security Annual Report

A Blueprint for Leadership in Security

EQUIFAX®

A Note from Equifax CEO Mark Begor

In April 2018 when I joined Equifax, I made a personal commitment internally and externally to building a culture within Equifax where security is a central part of our DNA and committed that Equifax would be an industry leader in data security. Since then, we've invested $1.5 billion to rebuild our company's security and technology infrastructure, and I am extremely proud of the incredible progress that we have made toward embedding security into everything we do – from our technology infrastructure, data fabric, and product development, to our merger and acquisition strategies, to our incentive compensation plans. As a data, analytics, and technology company, we are entrusted with sensitive consumer information, and we must do everything we can to protect it.

Equifax's commitment to security starts with our employees. Every employee – myself included – receives customized and required training in security, and throughout the year, we conduct various simulations to keep our skills sharp. We give employees direct visibility into their own security performance each month along with clear actions to improve their score. We even added a security component to our annual incentive plan for all bonus-eligible employees, becoming one of the first publicly traded companies to do so.

Over the past three years, we have hired hundreds of new cybersecurity professionals and built a global, 24x7, multi-million dollar detection and response center. We have built one of the industry's leading security teams globally. Our industry leading cloud technology transformation has made us more secure and enabled us to use our differentiated data assets to innovate and develop solutions, with built-in security, to better serve our customers and consumers.

Cybercrime – targeting individuals, our nation's businesses, and our government – is one of the greatest threats facing our nation today, and it is an ongoing battle that every company will continue to face as attackers grow more sophisticated. US corporations are continually fighting criminals that operate outside the rule of law and attempt to extract data for their own gain. These attacks no longer are just a hacker in the basement attempting to penetrate a company's security perimeter but instead are carried out by increasingly sophisticated criminal rings or, even more challenging, well-funded nation-state actors or military arms of nation-states. Continued investment in industry-leading data protection technologies and open collaboration to share best practices are our only defenses.

At Equifax, we firmly believe that security should not be a trade secret. We recognize that part of being an industry leader in data security is being transparent about our learnings and actively sharing the best practices that we are collecting as we work to implement change. We remain committed to working openly with our peers, customers, and partners to tackle emerging security challenges, document best practices, provide vital data security thought leadership, and work together to deliver solutions that benefit both the security community and consumers.

And while we have come a long way, we know there is more to do and that our efforts can't stop here. We are committed to putting security first and each of our more than 11,000 Equifax employees stands behind that commitment. We know that we must earn the trust of consumers and our customers every day by being an Industry Leader in Security.

MARK W. BEGOR
Chief Executive Officer, Equifax

A Note from Equifax CISO Jamil Farshchi

The cyber attacks we're seeing today are unprecedented.

This past year, we witnessed scores of ransomware attacks on hospitals, police departments, schools, and city governments. In electoral battleground states like Pennsylvania and Florida, foreign actors conducted email campaigns to intimidate voters and incite social unrest ahead of the 2020 US presidential election.

As we grappled with COVID-19, state-sponsored adversaries broke into the computer systems of pharmaceutical companies and research universities intending to steal coronavirus vaccine data.

Then came the SolarWinds breach. Sophisticated nation-state actors infiltrated vast segments of business and national security by exploiting an under-the-radar supplier. Just weeks later, we learned that Microsoft Exchange Servers used by thousands of organizations and millions of people were hacked.

Cybersecurity is no longer a looming threat; it's our daily reality. And, as our technology evolves – shifting and accelerating every aspect of our lives – it brings with it a new paradigm of cyber risk. The key here is that the challenges we face in cyber aren't relegated to large businesses or government agencies. This risk is universal. No matter your age, where you work, or where you live, no one is immune to these threats. We are all on the front lines.

Sunlight is the best disinfectant

Imagine taking your family out to dinner. Approaching the restaurant, you notice a sign on the door that reads, "Health Code Grade: F." You wouldn't step another foot forward. No one would. Today, there are no publicly available ratings that show how well companies are doing on security. And yet, we interact with businesses online and in-person every day without knowing how safe they really are.

If done properly, creating a common security standard would enable us to hold brands and businesses accountable before it's too late. It would incentivize them to invest in security and prioritize areas like privacy. And, it would make it easier for all of us – business, government, and the general public – to manage cyber risk.

I believe this type of security data should be public. So that's exactly what Equifax is doing. In this report, we're publishing how our company compares to other industries when it comes to security maturity, posture, and awareness – benchmarks that show how well an organization can adapt to cyber threats and manage risk over time. Our scores aren't perfect, but they are a step in the right direction and one that every organization should follow.

Knowledge drives behavior

Cybersecurity has an education problem. If consumers don't know how to spot threats, how can they protect their personal information or keep their identities safe? If corporate executives or board members don't understand cybersecurity, how will threats receive the right level of governance, oversight, and investment? If lawmakers aren't cyber savvy, how can they enact smarter and stronger cyber policy?

The lack of expertise in cyber hurts every business and government entity. Despite being among the highest-paying jobs, studies suggest that there are 3.5 million unfilled positions in cybersecurity today. If we want to win in cybersecurity, we need the talent. So, whether it's K-12 or higher education, there needs to be a renewed focus on cybersecurity curriculum in our schools and creating opportunities for more people to gain exposure to the field.

These steps will undoubtedly help us narrow the enormous gender and racial diversity gaps we have in security. Women comprise nearly half of the labor force in the US and nearly 40% worldwide, but in the security field, that number is only 24%. Black security professionals make up only 9% of the US security industry. We won't succeed if we aren't able to bring in talent from every corner of our population.

A seat at the table

Despite the fact that 85% of US critical infrastructure is owned by the private sector, business leaders aren't a part of the cyber conversation at the right levels of government.

One of the consequences of not having a seat at the table: valuable threat intel. The threat intelligence that cyber professionals get from the government today is typically limited, dated, and oftentimes inactionable. We need a pathway for the government to share with the private sector classified and unclassified information to the greatest extent possible. This intel is essential to national security and would put businesses on far better footing when defending against threats, especially in the heat of battle.

More broadly, the absence of meaningful collaboration leaves our true cybersecurity potential untapped. Much of the innovation and technical know-how resides within the business community. Private sector ingenuity has given us one-click retail and instant connectivity with friends and family. It's given us safer cars and safer medicine. It's created countless new jobs, powered millions of small businesses, and catapulted start-ups from college dorm rooms to the floor of the New York Stock Exchange. The examples are endless. We need that level of skill and imagination at the table alongside our leaders in government.

The fundamental act of working together isn't a silver bullet (spoiler: there is none), but partnership can be a vital tool in upping our capabilities – especially for small or medium-sized businesses who need to lean on the security expertise of others. We can't win in cybersecurity by operating solely within our own four walls. But, with a collective defense, I believe we can.

Choosing to fight

The reality is that every organization, large or small, is a target for a cyber attack. And, when a breach happens, how you respond matters.

Unfortunately, most companies that are breached will simply fix the issue and move on. This has become the norm, but it doesn't have to be. Our team chose a different path. Following the cyber attack on Equifax in 2017, we made a commitment to transforming our company's security from the top down; using our investments and expertise to help protect others; and collaborating with leaders in government and business to make society more secure.

Today's cyber challenges are unprecedented – and Equifax is ready. Few companies have invested more time and resources into ensuring that consumers' information is protected. But we can't win this war alone. We need more companies to lean in on cybersecurity. We need more people who are working every day to build better resilience, shape the legislative agenda, and share best practices.

We have the opportunity to usher in a new era of cybersecurity. I hope you will join us in this fight.

JAMIL FARSHCHI
Chief Information Security Officer, Equifax

Highlights

We embedded security into the DNA of Equifax.

- Invested $1.5 billion in security and technology, the largest investment in our 122-year history.
- Assembled a team of more than 600 highly-specialized security professionals.
- Changed our reporting structure, elevating the CISO role to report directly to the CEO.

We established a security-first culture.

- Added a security component to the annual incentive plan for all bonus-eligible employees – one of the first publicly traded companies to do so.
- Gave every employee visibility into their own security performance each quarter along with clear behaviors to improve their security scorecard.
- Strengthened our talent pipeline, increasing both our technical talent and our team's diversity.

We rebuilt our company's security and technology systems.

- Automated over 150 security checks in our cloud environment, giving us visibility into our security posture – in real time – to a degree that has never before been possible.
- Became one of the earliest adopters of the National Institute of Standards and Technology (NIST) Privacy Framework.
- Built a $7.3 million Cyber Fusion Center that supports 24-7 detection and response.

We leveraged our expertise to help customers become more cyber resilient.

- Embedded our leading security capabilities into the products and services we deliver.
- Combined advanced analytics and intelligent data orchestration to help businesses increase trust in digital identity.
- Launched CloudControl, a program that gives our customers unique visibility into the security of the cloud products they use.
- Created an unmatched, white-glove breach services program that helps companies better prepare for, defend against, and respond to attacks.

We made a commitment to become a force for good in security.

- Conducted over 100 lessons learned briefings with customer security teams and policymakers.
- Collaborated with think tanks, NGOs, and global organizations to advance cyber-related issues.
- Enhanced our collaboration with intelligence partners like the FBI and DHS.

A Transformation Unlike Any Other

THEN | 2017: A Cyber Attack by the Chinese Military

In 2017, Equifax discovered that cyber attackers had gained access to our network and the personal information of more than 147 million people. One study found that:

- an Apache Struts vulnerability was not properly identified as being present on a public website when patches for the vulnerability were being installed;
- an expired digital certificate contributed to the attackers' ability to communicate with compromised servers and steal data without detection;
- because individual databases were not segmented from each other, the attackers were able to access additional databases; and
- the attackers gained access to unencrypted credentials for accessing additional databases, which enabled the intruders to run queries on those additional databases.

"In the aftermath of a cyber attack by the Chinese military, we've transformed our security program from the top down, across every level."

Jamil Farshchi, Equifax CISO

NOW | 2021: An Elite Security Function Ready for Evolving Threats

Today, Equifax has an industry-leading security program, built with a $1.5 billion investment and backed by a team of more than 600 highly-skilled security professionals.

A security-first culture is the foundation of our success. Each year, 100% of our employees and leaders receive customized training, and throughout the year, personalized scorecards and simulations keep our skills sharp.

Our migration to the cloud has created an opportunity to exceed traditional on-premise security. Real-time visibility into the status of more than 150 security checks across our cloud environment is used by our teams to manage risk. And, our controls are supported by highly automated code scanning and patching.

Equifax's $7.3 million Cyber Fusion Center supports 24-7 detection and response, using state-of-the-art technology including behavioral analytics to counter fraud.

In the face of the challenge of cybersecurity, our team successfully defends against millions of threats every day – because we know that customers and consumers are counting on us.

Our commitment to transparency extends beyond our business. We collaborate with partners like the FBI and policymakers to improve security around the world. And, we use our lessons learned to build better solutions for our customers and consumers.

Our Guiding Principles

Our core beliefs about security defined how we approached our transformation and how we're moving forward.

1

Transparency builds trust.

Security is all about trust, and we set an expectation as an organization that we would build trust through transparency. That aim has driven us to give our customers visibility into the security of the cloud products they use and to share best practices with customers, competitors, and peers. We also actively collaborate with government agencies to share threat intelligence.

2

Culture is our foundation.

We've embedded security into our DNA. We started by establishing a expectation that security is everyone's responsibility – not solely the job of the security team. We reinforced that by adding a security measure to the incentive plan for all bonus-eligible employees, an approach that is unique among our peers. And we gave every employee visibility into their own actions in a security scorecard.

3

The cloud is the future of security.

Our cloud-first approach has enabled us to build better, stronger security. In the cloud, we are bringing to life our vision for real-time visibility into our security. Our developers use a library of patterns and stamps – reusable, security-approved building blocks that accelerate secure innovation and automation. And with continuous monitoring of over 150 cloud security checks, we ensure that secure configurations are applied across our cloud environments and applications.

4

Security is a competitive advantage.

Security is no longer a baseline requirement – it's a differentiator. That's why security leadership is part of our corporate strategy and why we have invested $1.5 billion in security and technology, the largest investment in our company's 122-year history. And because we know that prioritizing security starts at the top, we elevated the CISO role to report directly to the CEO, so that exceptional security is built into every strategic decision and product innovation.

Our Security Strategy

Over three years, we executed a strategy to build a strong foundation, mature our controls, and lead through trust and innovation.

2018 | ACT 1
Build

Talent
Capability Development
Compensating Controls

When we began our transformation journey we were faced with legacy infrastructure, a talent mix that skewed non-technical, and a reputation deficit to overcome. Our focus was on establishing a strong program by rapidly reducing risk in our environment while solidifying a sustainable team for the future.

2019 | ACT 2
Mature

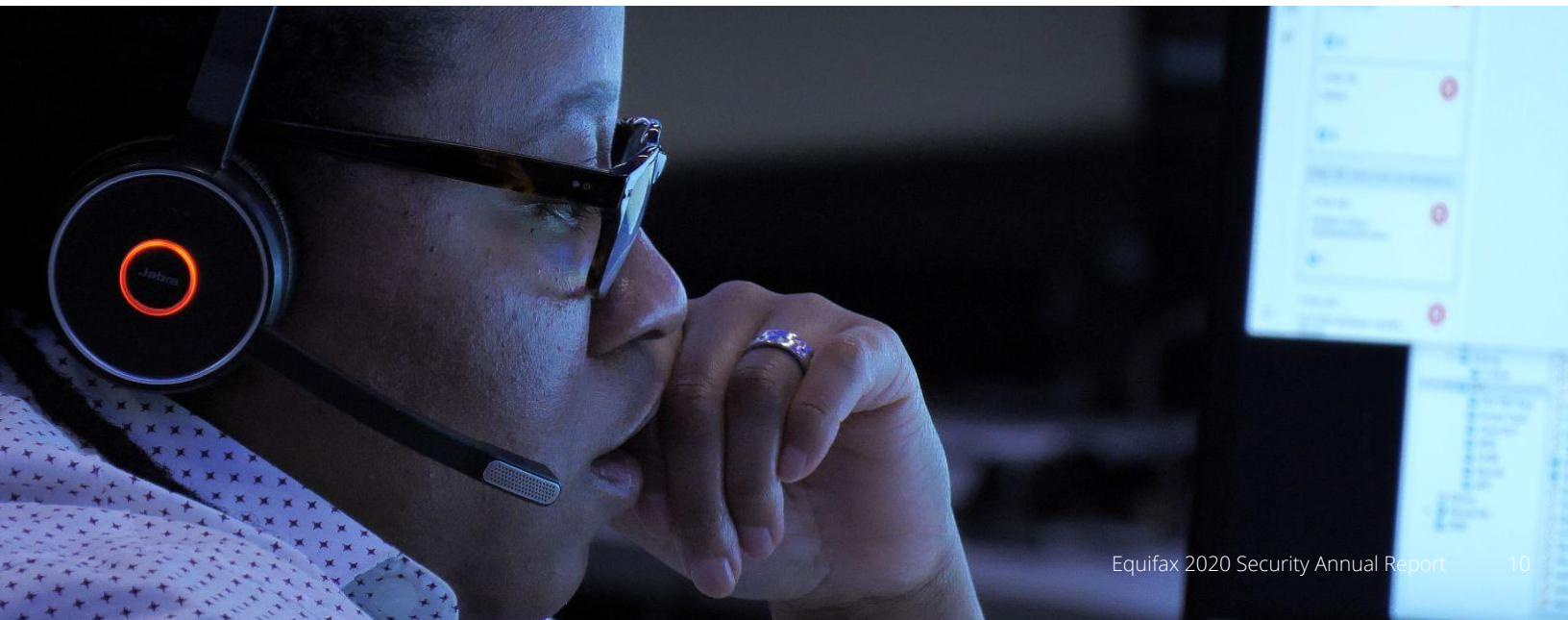
Cloud Foundation
Coverage Expansion
Regulations & Certifications

2019 was a year of execution. We made security a cultural norm. We worked with the Technology team to make cloud a reality and to embed security into development processes. We partnered with the external security community to help set and advance security standards. And we successfully regained certifications lost since the breach.

2020 | ACT 3
Lead

Risk Awareness
Capability Automation
Control Assurance

In 2020 we continued to execute our transformation, build trust, and pursue security leadership as we matured capabilities throughout our security program. We optimized our control environment, expanded automation to remediate weaknesses, and remained a strong contributor to the advancement of security worldwide.



Our Capabilities

Our team operates as one, bringing together core capabilities to protect those who rely on us.

Cybersecurity

The best offense is a good defense. We employ a defense-in-depth approach with multiple primary and compensating controls designed to prevent or limit the success of an attack.

Privacy

Cybersecurity and privacy go hand-in-hand. Privacy engineering is built into our development practices so that our products, services, and standards are created with privacy by design.

Fraud Prevention

Trusted digital transactions depend on knowing who is on the other side. Our advanced fraud prevention drives growth for Equifax as well as our customers and consumers.

Crisis Management

Regular tabletop exercises ensure we are ready to respond. Our strength in crisis management drove us to adapt quickly – and deliver our best year in history – during the COVID-19 pandemic.

Physical Security

Our comprehensive approach to security wouldn't be complete without protecting the 11,000 people in 24 countries who are behind the products and services we deliver.

Unified Controls

Industry-leading controls are central to our program, which is why we've contributed to new frameworks developed by NIST. In 2020, Equifax became one of the earliest adopters of the NIST Privacy Framework (PF), complementing our earlier adoption of the NIST Cybersecurity Framework (CSF). Today, our core capabilities – cybersecurity, privacy, fraud prevention, crisis management, and physical security – are represented in our unified controls framework.

Arming Our Customers

Collective security – a unified defense – is how we all win.

By using our security investments and expertise, we are helping our consumers and customers become more cyber resilient.

To do that, we leveraged our expertise in areas where we can make a real impact: trusted identity, supply chain security, breach services, and fraud detection.

Trusted Identity

Equifax combines advanced analytics and intelligent data orchestration to help businesses verify the identity of consumers and prevent fraud with pinpoint accuracy. Recently, we acquired Kount® to expand our global footprint. Kount uses AI to link trust and fraud data signals from 32 billion digital interactions and 17 billion unique devices across 200 countries and territories.

Supply Chain Security

To strengthen supply chain security for our business and our customers' businesses, we developed CloudControl – a platform that gives our customers visibility into the security of the cloud products they use. We're proud to be the first company in the world to make this technology available to our customers.

Breach Services

Equifax experienced the implications of a breach like few others have, and we want to help other firms build resilience against the digital threats we all face. Our unmatched white-glove breach services program has helped thousands of companies better prepare for and respond to attacks.

Fraud Detection

Equifax has used our investments to make personal security and fraud detection more transparent and convenient. Our ID Watchdog® product monitors consumer's credit and billions of data points, helping consumers stay informed of changes and activity related to their personal information. With myEquifax™, managing credit information online – including security freezes and fraud alerts – is easier. And we also built Lock & Alert® with a simple premise: consumers should be able to conveniently control access to their Equifax credit report, for life, and for free.

Our Progress

Independent benchmarking intelligence helps us gauge our progress.

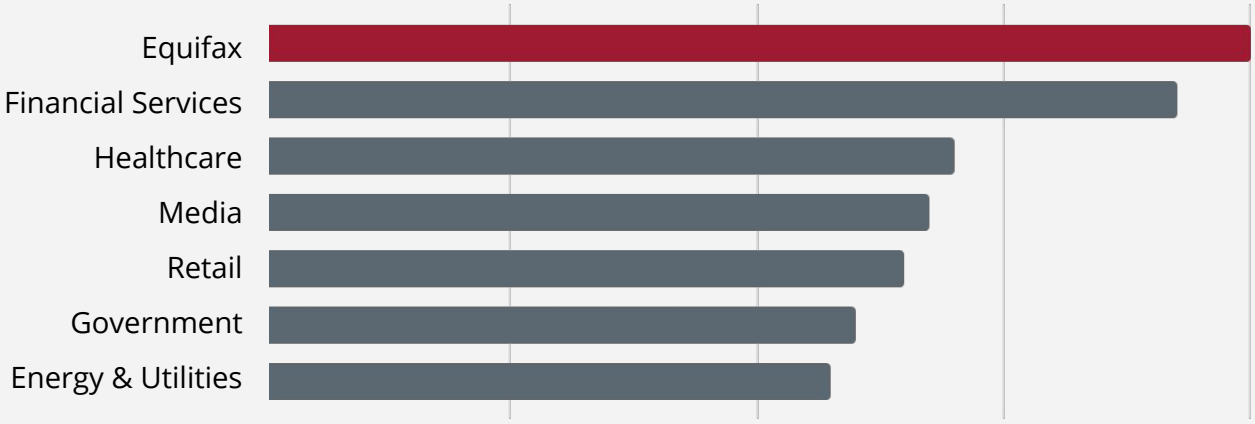
Equifax exceeds every major industry average on the Gartner Control Maturity Benchmark.

We used the Gartner Control Maturity Benchmark Service to assess our security program maturity. The chart below shows our score as well as average scores by industry, as published by Gartner. At year-end 2020, our security program outperformed the averages of 11 major industries.

What is Security Maturity?

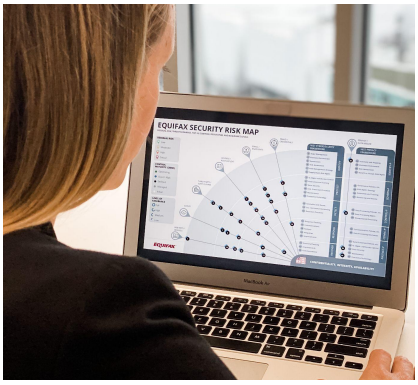
A set of characteristics or indicators that represents how well your organization can adapt to cyber threats and manage risk over time.

2020
Gartner Security Maturity Score



Graphic created by Equifax based on Gartner research. Source: Gartner, Inc., Control Maturity Benchmark Service, January 25, 2021.

Gartner makes no representations or warranties as to the source, or the compilation, of data input into the Gartner Controls Maturity Benchmark Service. Gartner disclaims all liabilities for any damages or penalties, whether direct, consequential, incidental or special, arising out of the use of, or inability to use, this material or the information provided herein. Clients may engage Gartner Consulting to help them complete and assess the results of this, and other similar, service(s).



A Force for Good

In the words of our CEO Mark Begor, "Security isn't a trade secret."

We're witnessing an evolution from mega to meta attacks. Our adversaries are shifting from targeting individual companies to using our interconnectedness to harm thousands with a single attack – a playbook that will continue to be effective until cyber defenders truly work together.

Protecting the data within our "four walls" is only part of the equation. Real leadership means taking bold steps both within and outside our organizations. To outpace our adversaries, we must work together to strengthen the security of our entire business ecosystem.

Security is an arms race. We must keep getting better – together. By leveraging our expertise, we can prepare – and help others prepare – to defend against emerging threats.

2020 Security Annual Report

Appendix

CAPABILITIES & CONTROLS

Cybersecurity

Developed a cloud assurance tool with real-time monitoring of over 150 cloud security checks.

Built a $7.3 million Cyber Fusion Center that supports state-of-the-art detection and response.

Implemented a 24-7 Security Operations Center.

Established a threat and vulnerability management program and policies, standards, and risk-based requirements that govern our patching processes.

Launched a platform for threat analysis with user behavior analytics to detect account exploitation.

Migrated from alert-based to threat-based Security Orchestration Automation and Response (SOAR).

Consolidated certificate management to a single authority that now renews public and private SSL certificates.

Vaulted over 70,000 privileged, administrative, and service accounts and manage privileges on over 30,000 endpoints.

Migrated over 20,000 users to improved multi-factor authentication (MFA) required for remote access.

Implemented a consolidated authentication platform securing over 500,000 authentications per month.

Upgraded our cloud proxy, which allows employees around the world to securely connect to the cloud.

Increased web application firewall (WAF) coverage across our network and implemented a consolidated platform for WAF management.

Implemented a DevSecOps program including penetration testing and full application code reviews.

Program Maturity

Developed a control framework aligned to the NIST Cybersecurity Framework and Privacy Framework.

Exceeded every major industry average on the Gartner Control Maturity Benchmark.

2020 Gartner Security Maturity Score

Graphic created by Equifax based on Gartner research. Source: Gartner, Inc., Control Maturity Benchmark Service, January 25, 2021.

Ranked in the top 3% of the of the 1,000 largest US firms surveyed by BitSight, a cybersecurity ratings company.

March 2021 BitSight Security Posture Rating

Outperformed the financial services industry median on the Gartner Secure Behavior Index, which measures employees' likeliness to act across a range of behaviors which impact the security of their organizations.

December 2020 Index of Secure Employee Behavior

Graphic created by Equifax based on Gartner research. Source: Gartner, Inc., Employee Awareness Service, December 2020.

Gartner makes no representations or warranties as to the source, or the compilation, of data input into the Gartner Controls Maturity Benchmark Service. Gartner disclaims all liabilities for any damages or penalties, whether direct, consequential, incidental or special, arising out of the use of, or inability to use, this material or the information provided herein. Clients may engage Gartner Consulting to help them complete and assess the results of this, and other similar, service(s).

Unless otherwise noted, information is as of March 2021

Crisis Management

Implemented COVID-19 safety and security protocols including enhanced threat monitoring.

Completed annual tabletop exercises with the Board of Directors and senior leaders.

Identified and trained regional crisis teams to effectively respond to incidents.

Fraud Prevention

Developed a custom Risk Assessment Engine that uses identity corroboration to detect the use of stolen credentials, account takeovers, synthetic identities, and other forms of identity theft.

Implemented real-time fraud prevention and monitoring.

Physical Security & Investigations

Supported law enforcement actions to combat fraud and identity theft.

Created a graduated response model to adapt our physical security response based on intelligence from local, state, and federal authorities.

Implemented AI-enabled physical security systems in our locations around the world.

Privacy

Built a dedicated privacy team led by our new Chief Privacy and Data Governance Officer.

Contributed to the NIST Privacy Framework.

Embedded privacy engineering into our development practices so that our products and services are created with privacy by design.

Built a comprehensive data inventory and regular enterprise update cycle.

Fully updated our data classification and handling requirements which govern the handling of data throughout our network.

Expanded encryption on data at rest and in transit.

COMPLIANCE

Certifications & Regulatory Compliance

Obtained re-certifications and compliance reports including PCI DSS, ISO 27001, SOC 1, and SOC 2 for applicable portions of our environment.

Maintained or established compliance with regulatory standards such as SOX, NYDFS, and FISMA for applicable portions of our environment.

Built compliance programs to address privacy regulations such as the California Consumer Privacy Act (CCPA).

Risk Management

Enhanced our security and technology integration process for acquisitions with additional penetration testing, vulnerability and code scanning, and compromise and threat assessments.

Enhanced oversight by enrolling over 3,000 suppliers and third parties into continuous risk monitoring.

CULTURE

Governance

Changed our reporting structure so that the CISO reports directly to the CEO.

Added Directors with technology and security expertise to the Board.

Developed Cyber Oversight Framework (COF) to communicate security risks and priorities to our Board of Directors and senior leaders.

Incentives & Training

Added a security goal to our incentive compensation plan for all bonus-eligible employees.

Provided security training to all members of our Board of Directors, leaders, and employees annually.

Deployed a security scorecard to employees globally.

Talent & Diversity

Assembled a team of more than 600 highly-skilled security professionals.

Increased the number of security team members with technical skills from 30% in 2018 to 79% in 2021.

Sponsored employees completing a M.S. in Cybersecurity and obtaining security certifications including SANS and CISSP.

Exceeded benchmarks for women (25% vs. 24% industry average*) and diversity (42% vs. 26% US industry average**) for US security employees.

*_The (ISC)² Cybersecurity Workforce Study: Women in Cybersecurity_, (ISC)², 2019
**_Innovation Through Inclusion: The Multicultural Cybersecurity Workforce_, Frost & Sullivan and (ISC)², 2018
Unless otherwise noted, information is as of March 2021

CUSTOMERS & CONSUMERS

Customer Engagement

Launched CloudControl, a program that gives our customers unique visibility into the security of the cloud products they use.

Conducted over 100 lessons learned briefings with customer, peer, and industry security teams.

Completed more than 10,000 audits, questionnaires, and other customer security inquiries.

Hosted Customer Security Summits in the US, Canada, and UK.

Products and Services

Embedded our leading security capabilities into the products and services we deliver.

Combined advanced analytics and intelligent data orchestration to help businesses increase trust in digital identity.

Created an unmatched, white-glove breach services program that helps companies better prepare for and respond to attacks.

Helped consumers stay informed of changes and activity related to their personal information with ID Watchdog®, myEquifax™, and Lock & Alert®.

Partnership & Collaboration

Continued supporting the FBI and the US Department of Justice, resulting in the indictment of 4 members of the Chinese military for the 2017 cyber attack.

Advanced cyber-related issues in collaboration with the World Bank, Cyberspace Solarium Commission, National Association of Corporate Directors, Organization of American States, and National Retail Federation.

Partnered with the Better Identity Coalition and international organizations to create a more secure digital future.

Shared updates on our transformation with outlets including *The Wall Street Journal, Bloomberg, The Hill, CNET,* and *Wired.*