EQUIFAX®

2021 Security Annual Report

Accelerating Our Leadership in Security

Security shouldn't be a trade secret. We believe that more communication, more collaboration, and more transparency, equals stronger security. That's why our team developed this report, and it's why we actively engage with customers, policymakers, and other organizations, regarding the challenges and opportunities in cybersecurity.

Our Impact

Equifax Security in 2021

35 million +	Cyber threats defended against on average each day
370,000 +	Simulations launched to test our global workforce in security
11,000 +	Employees received personalized security training
1000 +	Deep-dive risk analyses conducted on digital supply chain partners
800 +	Organizations supported through Equifax Breach Services
600 +	Cybersecurity professionals protecting consumer data
160 +	Automated cloud security checks monitored in real time
150 +	New Equifax products securely brought to market
50 +	Forums participated in to tackle global cyber challenges
20	Certifications and authorizations obtained from outside auditors
14	Tabletop exercises held to prepare for crisis scenarios
8	Acquisitions evaluated through robust risk assessments
0	Critical and high perimeter vulnerabilities outside of SLA

Mark W. Begor
Chief Executive Officer
Equifax

We are a New Equifax.

Over the past four years, we have transformed our organization at every level, investing $1.5 billion in technology and security to build the Equifax Cloud. We are truly a diversified data, analytics, and technology company that has expanded well beyond a traditional credit bureau – and we're just getting started.

When I joined Equifax in 2018, I made a personal commitment to establish Equifax as an **industry leader in data security** and to build a culture where security is part of our company's DNA. Since then, almost every aspect of our security program has been completely overhauled, and the results speak volumes. In multiple independent ratings, our security capabilities now exceed every major industry benchmark. We are 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.

Our commitment to world-class security is one of the key priorities in our Environmental, Social, and Governance (ESG) strategy, and we believe that our focus on ESG will better position our company for long-term sustainability and build shareholder value. Engagement in security spans every level of our organization: every employee at Equifax receives customized training in how to spot threats and has visibility into their own security performance. And every bonus-eligible employee has a security performance measure included in the calculation of their annual incentive compensation – helping them to understand how they contribute to protecting our systems and treat security as a personal priority. This reinforces our culture and aligns our employees with progress against our security program goals.

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, partners, and regulators 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 our customers. That is why we are sharing this Security Annual Report.

The strides we've made in cybersecurity – especially those from the past year that you'll read in this report – couldn't come at a more crucial moment. Attacks on companies, governments, and individuals, are more prevalent, more complex, and more impactful than ever. Alongside this, every organization is accelerating their reliance on technology, and consumers are engaging with digital touchpoints at levels never seen before.

All of this raises the stakes for data security, but Equifax is ready. We're proud to have built one of the most advanced and effective cybersecurity programs in business today, successfully defending against roughly 35 million cyber threats per day last year, around seven times more than in 2018. The cyber incident we experienced in 2017 was a catalyst to transform, and it led us to where we are today, earning recognition as a leading authority in security. **At Equifax, security has become a point of strength and a competitive advantage.** But, we are not done. We view security as a key differentiator and will continue to invest in security leadership.

Jamil Farshchi
Chief Information Security Officer
Equifax

Choosing action.

2021 was a watershed year in cybersecurity. We witnessed a record number of data breaches, a wave of ransomware attacks, penetration of digital supply chains, and disruption of our critical infrastructure.

To top it off, we concluded the year with a landmark Log4j vulnerability and the looming threat of a conflict between Russia and Ukraine.

Add in the macro backdrop of society's increasing technical dependence, innovation in areas like AI, Web3, and 5G, and the eye-popping financial returns that cyber criminals are generating, and it's indisputable that unprecedented levels of cyber risk are being unleashed upon us.

This is today's reality. Risk is both evolving and accelerating, and it's clear that maintaining the status quo in cybersecurity is untenable.

There's no shortage of options. We have in front of us an urgent list of to-do's in cybersecurity: new policy and regulation, better technology and innovation, more investment and collaboration, greater training and development. And yet, far too many organizations have chosen to remain in the status quo... to simply wait-and-see, to hope for the best.

This is a fatal risk miscalculation. Few (if any) corporate risks carry both the likelihood and impact as cyber threats do. Not only are attacks a certainty, successful ones consistently cripple business operations, generate crushing liabilities, and draw the ire of customers, investors, regulators, and the media. Hope is a dangerous risk management strategy.

But then, **there are others who choose action. Those who invest, innovate, and collaborate in ways that make their business and those around them more secure.** These firms know that what's been done before won't curb the trend line of successful attacks. They know that we have to constantly raise the bar in order to out-smart, out-work, and out-innovate cyber criminals. They embrace the reality that there is no finish line in security.

This has been the Equifax approach since the 2017 cyber attack on our company. We've elevated security in every facet of our business – from digital supply chain to M&A to new product innovation. Just as important, we continue to lean in on transparency, speak up, and help other organizations become more cyber secure.

Despite the challenges, threats, and uncertainty that exist in cyberspace, we remain committed to being a leader in Security. We've chosen action.

State of Play

Global Cybersecurity Threats in 2021

Organizations of every size and industry are dealing with a proliferation of security challenges around the world.

That's why we created the Threat Condition Framework. Our team tracks the rapidly evolving cybersecurity landscape and takes these real-world events into account when evaluating our Enterprise Threat Level.

Equifax Threat Condition Framework

Equifax Security manages our Enterprise Threat Level which adjusts based on a range of factors. For each threat level – Guarded, Elevated, High, Severe – we have a series of predefined processes that activate various actions from our team. Our Enterprise Threat Level is regularly reported to the company's Senior Leadership Team and Board of Directors.

- Severe
- High
- Elevated
- Guarded

The themes referenced below encapsulate the top macro situational awareness threats we witnessed in 2021.

Record number of data breaches

Data breaches in 2021 surpassed prior year levels[1] and proved once again that everyone is a target. However, in a sea of breaches, one stood out from the rest: a massive hack of Microsoft Exchange, one of the most popular email software programs in the world. The incident raised alarm from The White House who warned that organizations had "hours, not days" to fix vulnerabilities. The breach was so severe that it prompted the FBI to obtain a court order enabling the agency to proactively access and patch infected computers across the United States.

Powerful surge in ransomware attacks

Ransomware has been around for decades, but in 2021, attacks on organizations, cities, and individuals, hit unprecedented levels. The world's largest meat supplier, a consulting behemoth, an insurance giant, and a major payroll provider, were all held for ransom. One company paid a record-breaking $40 million to cyber criminals. The volume of suspected ransomware payments flagged by U.S. banks nearly doubled from 2020. The string of attacks prompted officials from more than 30-nations to convene an international summit to address the crisis.

Unprecedented cyber incidents on critical infrastructure

No ransomware event garnered more headlines than the attack on Colonial Pipeline, the operator of the largest fuel pipeline in the U.S. The cyber incident caused panic across the East Coast and spiked gas prices to their highest level in seven years. For the first time, cybersecurity became a reality for millions of people. Across the Atlantic in Ireland, a separate cyber attack paralyzed the country's entire healthcare system, which provides care to 5 million people. It was a devastating attack as patient data and computer systems were held ransom for weeks.

New software vulnerability wreaks havoc

A flaw found in widely used open-source code known as Log4j impacted seemingly every major business, organization, and government entity on Earth. The vulnerability was easily exploited and put hundreds of millions of endpoints and servers at risk. One security firm found that there were more than 100 hacking attempts to exploit the vulnerability every minute. Among the victims was Belgium's Defense Ministry, which was forced to shut down parts of its computer network after discovering a cyber attack involving Log4j. One U.S. cybersecurity official called Log4j "the most serious vulnerability seen in their career."

[1]Identity Theft Resource Center, 2021 Data Breach Report

Our Actions

Equifax Security Initiatives and Results in 2021

Expanded Our Cloud Security

We enhanced our top-tier cloud security to include automated validation and monitoring. Our migration to the cloud gives us more robust visibility into the security of our enterprise, which in turn enables us to detect and respond to threats with more speed and precision.

In 2021, we implemented more than 160 automated cloud security checks that are now monitored in real time.

Enhanced Our Employee Training

We further customized our employee security training program and fully automated the delivery of behavior-based learning to meet the needs of our global business. Recognizing the unique threat of digital social engineering attacks, we accelerated that training by adding emotional triggers in more than 370,000 simulations we conducted in 2021. This enabled us to vary the difficulty of our training and ensure that our workforce remains skilled in security.

In 2021, our employee security awareness score reached a new record of 98 out of 100, a sizable improvement from 81 out of 100 in 2020. Additionally, our employees achieved a 4.7% simulation click rate, a 110% improvement from 2020.

Fortified Our Digital Supply Chain Security

We secured our digital supply chain with greater detail, speed, and innovation. Despite the complexity and unpredictability of most organization's supply chain management, our team is able to more effectively evaluate the security capabilities of the more than 5,000 vendors who support Equifax. This isn't the norm in risk management, but it's a great example of how we're protecting the entire ecosystem of our business.

In 2021, we conducted assessments on 100% of our company's vendors as well as deep-dive risk analyses on more than 1000 of our most critical digital supply chain partners.

Our Actions :: Equifax Security Initiatives and Results in 2021

Strengthened Our Global Risk Posture

We expanded our collection of specific security metrics for each of the countries in which we operate in order to strengthen our global risk posture. Our team now analyzes unique security risk measures at a regional level such as agent coverage, logging coverage, asset inventory accuracy, application code scanning, and certificate lifecycle management.

In 2021, we achieved improved rates of 88% agent coverage, 88% logging coverage, 98% asset inventory completeness, 71% of applications enrolled in automatic code scanning, and 98% certificate lifecycle management, across our non-U.S. geographies.

Advanced Cybersecurity Transparency

We continued to engage with stakeholders around the world – executives and policymakers, academics and intelligence officials, trade associations and small business owners – to advocate for stronger cybersecurity. By leveraging our expertise and sharing best practices, we're helping others prepare for and defend against emerging threats.

In 2021, we participated in more than 50 forums to advance ideas and solutions to global cybersecurity challenges, including engagements with the Federal Bureau of Investigation, U.S. Department of State, National Technology Security Coalition, and World Economic Forum.

Enabled Business Growth

We helped our business drive more innovation, more securely. Our Security team collaborated across the enterprise to bring to market a record-number of new products and unlock new commercial opportunities for our company. These efforts made clear that good security isn't just about combating attacks – it's also an enabler of driving bottom line results.

In 2021, we helped securely bring to market more than 150 new products for Equifax customers, launched a state-of-the-art FedRAMP security environment to support the U.S. government in the cloud, and drove new business in areas like identity and fraud.

Furthering Our Security Transformation

In 2017, Equifax faced one of the most consequential cyber attacks in history when members of the Chinese Military gained access to our network and the personal information of more than 147 million people.

Today, there's little if any aspect of our security program that hasn't been completely overhauled from what was in place in 2017.

Few companies have dedicated more time and resources into ensuring consumer information is protected. But, we're not stopping here. Our team is committed to constantly raising the bar in security by:

Investing
in top-tier cybersecurity capabilities and building a security-first culture

Innovating
in ways that make our business, our customers, and consumers, more secure

Collaborating
with others in order to be a force for good in cybersecurity

We've transformed our security program across every level.

Invested $1.5 billion to rebuild our technology and security capabilities from the ground up

Migrated our enterprise to the cloud, giving us stronger visibility into the data coming in and out of our environment

Built a $7.3 million Cyber Fusion Center that supports 24/7 detection and response

Hired more than 600 highly-skilled cybersecurity professionals to respond to threats with speed and precision

Changed our organizational structure by elevating security to report directly to our CEO

Strengthened the way our Board members assess key risk areas across business

Instituted a rigorous employee security training program with monthly simulations and individualized scorecards

Embedded automated validation and monitoring of more than 160 cloud security controls in real time

Launched a state-of-the-art FedRAMP security environment to support U.S. government customers in the cloud

Enrolled more than 3,000 suppliers and third parties into continuous risk monitoring

Developed CloudControl, a platform that gives customers real-time visibility into the security of their Equifax Cloud products and services

Acquired Appriss Insights, a leading source for risk and criminal justice intelligence, and Kount, a global leader in digital identity and fraud solutions

Obtained certifications and authorizations including PCI DSS, ISO 27001, SOC 1, SOC 2, and FISMA

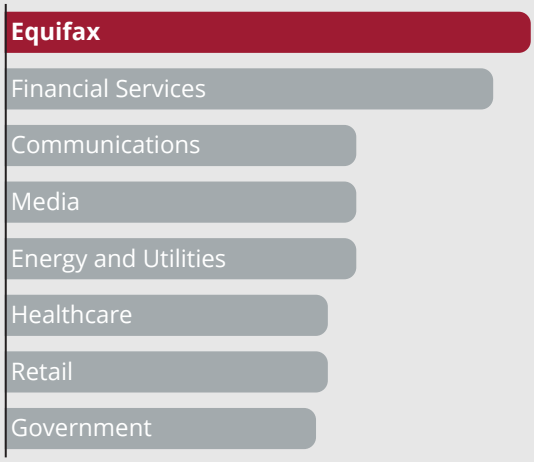
Independent Benchmarking

Security Maturity

A leading global research and advisory firm conducts annual in-depth analysis of the maturity of our entire security program.

What is Security Maturity?
An organization's security maturity represents how well it can adapt to cyber threats and manage risk over time.

2021 Security Maturity Score



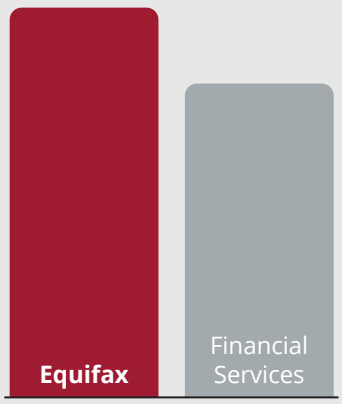
At year-end 2021, the maturity of our cybersecurity program outperformed all major industry benchmarks for a second consecutive year.

Security Posture

A leading cybersecurity reporting service continuously monitors the posture of our security program and assesses the risk of our supply chain ecosystem.

What is Security Posture?
An organization's security posture is its readiness and ability to identify, respond to, and recover from security threats and risks.

2021 Security Posture Rating



At year-end 2021, our security posture ranked in the top 1% of Technology and Financial Services companies analyzed.

Summary of Results

Equifax Security in 2021

Security Maturity and Posture	• Optimized cybersecurity spend as a percentage of IT budget to 10%, below the industry average of 10.6%[2] • Achieved a Security Maturity score that outperformed all major industry benchmarks for a second consecutive year • Achieved a Security Posture rating that ranked in the top 1% of Technology and Financial Services companies analyzed
Cybersecurity	• Implemented more than 160 automated cloud security checks that are monitored in real time • Maintained 0 critical and high perimeter vulnerabilities outside our Service Level Agreement (SLA) • Expanded automated code scanning to 92% of our applications (vs. 54% in 2020) • Enforced Multi-Factor Authentication (MFA) for 100% of remote access to our network
Compliance	• Obtained 20 certifications and assessments from outside auditors validating our compliance with business, legal, contractual, and regulatory requirements, including: – PCI-DSS: Payment Card Standards – ISO 27001: Security Management Controls – SOC 2: Security, Availability, and Confidentiality Report – SOC 1: Audit Controls Report
M&A	• Conducted robust due diligence on 8 acquisitions, including comprehensive vulnerability scanning, code review, and compromise assessment, prior to closing • Led remediation and integration efforts for every acquisition to ensure new entities are operated in alignment with our core controls • Of note, facilitated two of the five largest acquisitions in Equifax history: Appriss Insights, a leading source for risk and criminal justice intelligence, and Kount, a global leader in digital identity and fraud solutions
Risk Management	• Conducted assessments on 100% of our company's vendors • Conducted deep-dive risk analyses on more than 1000 of our most critical digital supply chain partners • Onboarded several new customers to CloudControl, an industry-first platform which gives customers real-time visibility into the security of the Equifax Cloud products and services they consume

[2]IANS and ARTICO, 2021 Security Budget Benchmark Study

Summary of Results :: Equifax Security in 2021

Crisis Management	• Conducted 14 tabletop exercises and real-time crisis simulations with company stakeholders. Key stakeholders included: – Board of Directors – CEO and Executive Team – Regional and Business Unit Crisis Teams • Revised our Emergency Response Program framework
Security Training	• Conducted more than 370,000 simulations to test our workforce in security • Generated personalized security scorecards for every employee each month to educate our workforce in their cybersecurity performance • Increased employee security awareness score to 98 out of 100 (vs. 81 in 2020) • Reduced employee simulation click rate to 4.9% (110% improvement vs. 2020)
Breach Services	• Supported more than 800 organizations and their customers, helping them respond to and recover from cyber incidents
Customer Engagement	• Completed more than 1900 questionnaires and audits on behalf of Equifax customers to ensure compliance • Held Customer Security Summits and Roundtables in Australia, Canada, and the U.K., to further transparency
Products and Services	• Launched a state-of-the-art FedRAMP security environment to support the U.S. government in the cloud • Securely brought 151 new products to market for our customers (vs. 134 in 2020)
Privacy	• Launched a new, risk-based Privacy Impact Assessment process in the U.S. and Canada • Designed and implemented a governance process for privileged data zones • Deployed a new tool to support data discovery across the enterprise, enabling us to better triage, manage, and protect our data
Fraud	• Continued to evolve our Risk Assessment Engine, beginning our transition away from hard-coded decisioning logic and into models coupled with dynamic risk attributes

Summary of Results :: Equifax Security in 2021

Physical Security and Investigations	• Completed 8 physical penetration tests to identify areas of continual improvement in preventing unauthorized facility access • Completed 39 physical security assessments validating appropriate controls are in place to protect employees, data, and assets • Through enhanced processes and automation, our Physical Security Operations Center bolstered our response time for: – Local high priority alarms: within 4 minutes – Inbound intelligence reports: within 5 minutes • Mitigated/removed $1.3 billion in identified fraudulent reported consumer and commercial tradelines
Talent and Diversity	• Continued to grow diversity among our workforce by reaching: – 26% Women team members in the U.S. (vs. 24% industry average[3]) – 17% Black team members in the U.S. (vs. 9% industry average[3])
Advocacy and Partnership	• Participated in more than 50 forums to promote stronger cybersecurity for business, government, and society • Strengthened partnerships with law enforcement in combating fraud, identity theft, and identifying criminal activity • Collaborated with organizations to advance ideas and solutions to global cybersecurity challenges, including the: – Atlantic Council – Foundation for Defense of Democracies – Federal Bureau of Investigation – National Technology Security Coalition – U.S. Department of State – World Economic Forum • Released inaugural Security Annual Report, part of our ongoing commitment to further transparency in cybersecurity

[3]Aspen Institute, 2021 Diversity, Equity, and Inclusion in Cybersecurity Report

There's No Finish Line in Security

Our Priorities in 2022

Optimizing Our M&A Pipeline

M&A remains an important pillar of the EFX 2023 growth strategy, and Security is responsible for assessing the security risk of each and every acquisition target. As the M&A landscape evolves, we're seeing larger deal volume, more competition, and shorter diligence windows.

As we continue to accelerate our strategic M&A, we're leveraging new tools and optimized processes that enable us to identify any red flags, remediate threats more quickly, and streamline the integration phase.

Advancing Even Stronger NextGen Cybersecurity Technology

When it comes to securing our enterprise, we are committed to constantly raising the bar. That's why we're working with innovative leaders in the security space as design partners to help raise our core cybersecurity capabilities to even greater heights.

This next generation cybersecurity technology leans heavily on AI, cloud, and automation. Ultimately, this will enable us to gather better intel, detect and stop threats with greater speed, and reduce risk to our business.

Accelerating Frictionless Security

We're embedding self-serve and automation across our business. Why? Because our teams shouldn't have to choose between better security and stronger innovation. We can have both.

By introducing things like real-time risk decisioning, streamlined code scanning, and continuous supply chain monitoring, we'll be able to maintain our security leadership while placing less burden on our employees.

equifax.com