EQUIFAX®

2022 Security Annual Report

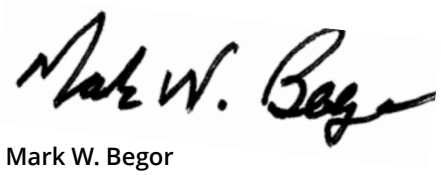
Table of Contents

A Message from
Equifax CEO
Mark W. Begor

The Next Gear of Cybersecurity

2022 was a strong year for the New Equifax as we shifted from an era of building the Equifax Cloud™ to securely leveraging the Cloud for innovation, new products, and growth. We have truly become a diversified data, analytics and technology company that has extended well beyond a traditional credit bureau in the 24 markets we serve worldwide. And, as we have grown and innovated to meet the evolving needs of global consumers and customers, we have also committed to partnering with them in new ways.

Cybersecurity is critical to that partnership.



Mark W. Begor
Chief Executive Officer
Equifax

When I joined the company 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 global team's DNA — where everyone in Equifax owns security. We have transformed our organization at every level to deliver on that promise. From our employee engagement, technology infrastructure, data fabric and product development, to our merger and acquisition strategies, security has become embedded in everything we do.

Over the last five years, we have built one of the world's most advanced and effective cybersecurity programs. Our maturity level has exceeded all major industry benchmarks, and our posture has ranked in the top 1% of Technology companies and top 3% of Financial Services companies analyzed, for three consecutive years.

Transparency has been critical to the growth and strength of our security program. We believe that more communication, more collaboration, and more transparency, equals stronger security. Actively sharing the best practices we've gained as we work to implement change is why we developed this report, and why we have continued to actively engage with customers, policymakers, and other organizations, regarding the challenges and opportunities in cybersecurity on a daily basis over the course of the last year.

2022 saw a host of new threats to global cybersecurity infrastructure. Equifax responded, defending against 39 million cybersecurity threats each day while conducting more than 374,000 simulations to test our global workforce and prepare for what's ahead.

While I'm energized by our progress, we're not done. The Next Gear of Equifax Security is one that comes with continuous evolution and an unwavering commitment to helping our customers, partners, and consumers strengthen their own cybersecurity postures for the benefit of the industry at large as Equifax drives for industry leadership in security.

A Message from
Equifax CISO
Jamil Farshchi

Shaping the Future

Half a decade. Feels like a blip and an eternity all at once. I joined Equifax five years ago and set forth a "MinMax strategy" for our security program — minimizing cyber risks while maximizing business growth. This strategy had three acts: Build > Mature > Lead.

It worked. We've achieved security leadership — and this report shows it. We still have cyber risk (we always will), but it's now being managed by top-tier talent, armed with next-gen technology and overseen by best-in-class governance. Just as importantly, we've done it while underpinning the most significant period of growth in our 124 year history. Good security IS good for the bottom line!

So what's next? What comes after "Lead"? One word: **Shape.**

We are actively working to help shape security behaviors, technologies, and practices beyond our four walls. Why? Because we're all heavily interconnected and reliant on each other. The old "you're only as strong as your weakest link" axiom is truer today than ever. It's simply not good enough for Equifax to be a leader in security — we ***all*** need to be.

The 2022 threat landscape underscored this imperative. Vulnerable infrastructures. An accelerating cyber arms race. Emboldened nation states. Over 50% of security incidents attributed to supply chain breaches. These are challenges none of us can solve alone.

Our answer to this is partnership. We established a bold vision to address some of security's most intractable challenges, and we worked cooperatively to chip away at them.

We enlisted security vendors to build our designs for next-gen training, supply chain, and cloud identity technologies. We teamed up with the Federal Bureau of Investigation (FBI) to improve public/private partnership. We shared our board partnership blueprint to promote corporate governance best practices. We joined business, government, and nonprofit leaders to educate global stakeholders about top cyber risks. And we're just getting started.

This is the way. Cooperation is the force multiplier that enables us all to win the cyber arms race. We owe it to each other, to our countries, and to our communities.

2022 was a challenging year in cybersecurity, and 2023 will certainly bring us surprises. But together, we can win this fight. Let's move forward with a shared commitment to make a difference.

Jamil Farshchi
Chief Information Security Officer
Equifax

Our Impact

39M +	Cyber threats defended against on average each day
374,000 +	Simulations launched to test our global workforce in security
23,000 +	Employees and contractors received personalized security training
2,700 +	Questionnaires and audits completed on behalf of Equifax customers to ensure compliance
750 +	Deep-dive risk analyses on critical risk third party vendors
600 +	Cybersecurity professionals protecting consumer data
280 +	Customers onboarded to real-time cloud security visibility dashboard
160 +	Automated cloud security checks monitored in real time
110 +	New Equifax products securely brought to market
40 +	Forums participated in to tackle global cyber challenges
38	Certifications and authorizations obtained from outside auditors
38	Physical security assessments completed, validating appropriate controls
14	Tabletop exercises held to prepare for crisis scenarios
4	New acquisitions evaluated through robust risk assessments
3	Consecutive years achieving a Security Maturity score that outperforms all major industry benchmarks

State of Play

The themes referenced below encapsulate the top macro situational awareness threats we witnessed in 2022.

Large-scale attacks on nations

Albania. Australia. Costa Rica. Estonia. Finland. Montenegro. Country after country felt the brunt of attacks on its infrastructure. This reality shows just how brazen bad actors have become — going after entire governments and damaging public utilities, trade and healthcare. But nothing seemed greater than the cyber assault on Ukraine that deployed everything from wiper attacks to hacking edge devices.

Supply chain vulnerabilities

Most companies have hundreds of digital supply chain partners. And last year saw a huge surge in third party attacks, which ultimately impacted over 10 million people. This unequivocally demonstrated that, if one weak link is compromised, the consequences can reverberate through many integrated organizations.

MFA bypass attacks

Multi-factor Authentication (MFA) has long been a "go-to" control in defenders' arsenals. Lately, its limits are being tested. Whether through social engineering tricks or brute force exhaustion, cyber criminals have found ways to bypass MFA.

Talent scarcity

With a global shortage of over three million cyber security workers, defenders found themselves outmanned in 2022. This talent shortage was complicated by the uptick in surface area to protect due to increased digitization. On a positive note, this conundrum pushed cybersecurity operations centers toward breakthroughs in efficiency, leveraging artificial intelligence and automation to fend off attacks in lieu of extra personnel.

The security landscape continues to evolve at a dizzying pace.

We stay ahead of it using the Equifax Threat Condition Framework. Our team stays abreast of the quickly changing cybersecurity scene, factoring these real-world events into the calibration of our Enterprise Threat Level.

Equifax Threat Condition Framework

Equifax Security manages our Enterprise Threat Level which adjusts based on a range of factors such as the rate at which other technologies are being compromised. 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 and has remained guarded throughout 2022.

- Severe
- Elevated
- High
- Guarded

Our Actions

Expanded Our Cloud Security

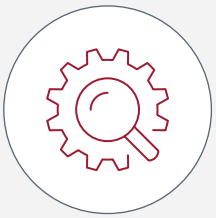
We continued to strengthen the security posture of the Equifax Cloud, achieving multi-cloud environment security parity and improving container security.

We also architected a Global Network Security Stack (GNSS), which establishes a standardized network security design and enables faster application onboarding and customer response time for critical cloud applications.

Strengthened Employee Security Awareness

We expanded our Security Scorecards to include Equifax contractors, ensuring the same high standards across our workforce. And we partnered with our training service provider to co-develop new, targeted measurements of key behaviors.

As one example of our workforce's increased cybersecurity awareness, employees are increasingly not clicking the phishing simulation emails we send, while also reporting them at a higher rate (and thus reporting more real phishing emails as well).

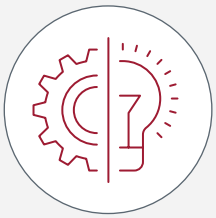


Optimized Our M&A Pipeline

Equifax continues to re-invest our strong performance in strategic, bolt-on acquisitions to strengthen our company and drive future non-mortgage growth.

The security team has enhanced our acquisition processes by establishing tiered control priority, a subset of key controls, and risk-based reporting. To ensure that newly-acquired businesses align with our rigorous standards, we completed controls alignment for 15 acquisitions.

Our Actions continued



Modernized and Connected our Security Tools

To increase our team's operating leverage, we uplifted our security toolset in the areas of endpoint protection, access management, logging and image recognition. The result is better governance, reduced risk and less friction for the business.

Much of this uplift was achieved through partnering with technology providers to co-design solutions that are now available to the market at large, strengthening security across the broader business ecosystem.

Enabled Business Growth

We onboarded 280+ customers onto CloudControl, a dashboard designed for our customers that provides real-time insights into the security posture of the Equifax Cloud-based products and services they use.

And, we obtained new certifications that create opportunities for the business, including earning U.S. Health Insurance Portability and Accountability Act (HIPAA) compliance for two key environments and obtaining Secret Facility Security Clearance from the Government of Canada.

Advanced Transparency and Collaboration

We built on our continued engagement with stakeholders around the world, prioritizing the topics and partnership opportunities that have the greatest impact on advancing cybersecurity.

This included sharing our expertise on forging effective board/CISO partnerships and facilitating effective dialogue between public and private organizations, partnering with organizations such as the Bipartisan Policy Center, the Swiss Cyber Institute and the National Association of Corporate Directors.

Shaping the Future

Security at scale requires teamwork. In 2022, we collaborated externally from multiple angles.

We had a strategic vision for our program and security at large, but no products existed to bring this vision to life. This didn't stop us. **We took our vendor relationships from transactional to transformative**, working side-by-side to bring next-gen solutions to market. Beyond shaping our own leading capabilities, these partnerships drive the entire industry forward.

- We sought a positive and motivating mechanism to target, educate, measure and incent a compendium of **secure employee behaviors**. So we partnered with our training vendor to improve the depth and breadth of their offering, including comprehensive measurement and real-time feedback.
- No product met our vision for how **supply chain security** should be done. So we helped build one, partnering with a software provider to transform a nascent product into a groundbreaking customer cloud transparency tool.
- We wanted a unified, cloud-based **identity governance and administration (IGA) and privileged access management (PAM)** solution. None existed. So we worked with a design partner to shape a solution, helping ensure integrated, next-generation, cloud-first capabilities — not just for us, but for everyone else in the market thereafter.
- We worked with the Ping Identity engineering team to automate our **authentication capabilities** and were recognized with their Cloud Identity Champion award for our "work that pushes our industry forward."

To help directors improve dialogue with CISOs and better understand cyber risks, we **shared our board partnership blueprint** with these groups:

National Association of Corporate Directors	The New York Stock Exchange (NYSE) Board Advisory Council	Glass Lewis Investors Perspective	Gartner Security & Risk Management	EY Audit Committee Network

And we engaged with legislators, government agencies, and regulators:

- Equifax CISO appointed as a **Strategic Engagement Advisor to the FBI**.
- Partnered with the **Bipartisan Policy Center** to highlight top risks in cybersecurity for business, government, and society in 2023.
- Partnered the **Costa Rica Cyber Security Cluster** to foster public-private partnership among the Ministry of Science and Technology, Costa Rican Chamber of Industries, universities, and other businesses.
- Contribute to policies in Chile via the **Chilean Cybersecurity Alliance**.
- Supported the cyber resilience of Australia and New Zealand via **CISOLens**.

Cyber Governance

Increased regulatory focus on cyber governance is turning security into a core responsibility of the board and management team.

And since we already have a strong partnership with our C-suite and Board of Directors, we're sharing our hard-earned learnings — both to help shape regulations and to help organizations comply.

Under the latest New York State Department of Financial Services (NYDFS) regulation, **the CEO and CISO must co-sign an annual attestation of security compliance,** and a corporate board must:

- Have significant cyber risk expertise and knowledge for effective oversight
- Approve a company's security policies, procedures, and risk assessment
- Receive briefings from the CISO, at least annually
- Review any material issues that arise from vulnerability assessments and penetration tests

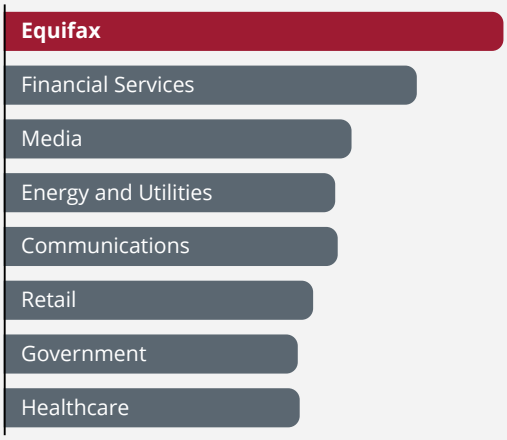
Investor advisory services leader Glass Lewis heralded our transparency as **"quite unique and remarkable."**

Independent Benchmarking

Security Maturity

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

2022 Security Maturity Score



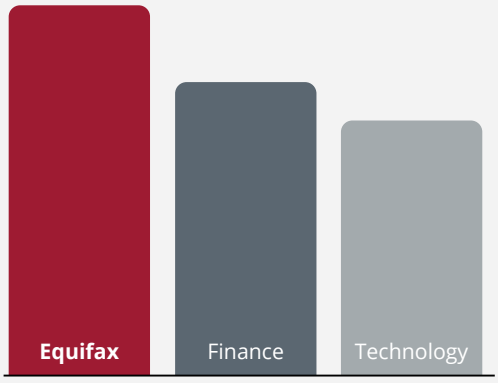
What is Security Maturity?
An organization's security maturity represents how well it can adapt to cyber threats and manage risk over time.

At year-end 2022, the maturity of our cybersecurity program outperformed all major industry benchmarks for a third 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.

2022 Security Posture Rating



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.

At year-end 2022, our security capabilities ranked in the top 1% of Technology companies and top 3% of Financial Services companies analyzed.

Summary of Results

Security Posture and Maturity	• Optimized cybersecurity spend to 9.2% of IT budget, below the industry average of 9.9% • Achieved a Security Maturity score that outperformed all major industry benchmarks for a third consecutive year • Achieved a Security Posture rating that ranked in the top 1% of Technology companies and top 3% of Financial Services companies analyzed
Cybersecurity	• Implemented 349 automated cloud security checks that are monitored in real time • Strong improvement in application security; 96% of verified apps were enrolled in automated scanning by the end of 2022 (versus 69% in August) • Enforced Multi-factor Authentication (MFA) for 100% of remote access to our network • Upgraded to next-generation tooling across endpoint protection, access management, logging, and image recognition
Compliance	• Obtained 38 certifications from outside auditors (a 45% increase over 2021) validating our compliance with business, legal, contractual, and regulatory requirements • Equifax Canada obtained the Secret Facility Security Clearance from the Government of Canada • Achieved HIPAA compliance for two key environments: Kount (our fraud protection platform) and our Breach Services business
M&A	• Conducted robust due diligence on the four acquisitions completed in 2022, including comprehensive vulnerability scanning, code review, compromise assessment, and key control reviews prior to closing • Developed a new three-tiered security integration strategy, ensuring new entities are aligned with Equifax controls without delay • Completed security control integration of 15 Equifax acquisitions
Risk Management	• Conducted deep-dive risk analyses on 100% of our company's critical risk third party vendors (750+) • Onboarded over 280 customers to CloudControl, an industry-first platform which gives customers real-time visibility into the security of the Equifax Cloud products and services they use
Crisis Management	• Conducted 14 tabletop exercises and real-time crisis simulations with company stakeholders. Key stakeholders included: – Board of Directors – CEO and Executive Team – 12 Regional and Business Unit Crisis Teams
Privacy	• Published the Privacy Engineering Handbook • Implemented Google Workspace Client-Side Encryption to encrypt sensitive data stored in Google Workspace

Summary of Results continued

Security Training	• Conducted 15 global and 18 targeted simulations to test our workforce in security • Expanded our Security Snapshot to 23,500 Equifax employees and contractors • Maintained a market-leading aggregate security score of 91, outperforming all major industry benchmarks • Reduced average employee phishing simulation click rate to 4.2% (10% improvement vs 2021) • Introduced new role-based behaviors into employees' Security Scorecard, including secure browsing and sensitive data handling
Breach Services	• Supported 716 organizations and their customers, helping them respond to and recover from cyber incidents
Customer Engagement	• Completed more than 2700 questionnaires and audits on behalf of Equifax customers to ensure compliance
Products and Services	• Securely brought 113 new products to market for our customers • Embedded strong product security enablement into the design stage of development cycle, advising product teams and empowering developers with a self-service tool to find and fix vulnerabilities
Fraud	• Introduced leading edge anti-fraud capabilities that incorporate machine learning, artificial intelligence and enhanced vendor inputs, while minimizing consumer friction
Physical Security and Investigations	• Completed 12 physical penetration tests to identify areas of continual improvement in preventing unauthorized facility access • Completed 38 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 3:21 minutes (16% faster response than 2021) – Inbound intelligence reports: within 2:07 minutes (58% faster response than 2021)
Talent and Diversity	Continued to grow diversity among our workforce: • 13% Black security team members in the U.S. (vs. 9% industry average) • 27% of security team members in the U.S. identify as female (vs. 24% industry average)
Advocacy and Partnership	• Participated in more than 40 forums to promote stronger cybersecurity for business, government, and society • Partnered with the Bipartisan Policy Center to highlight top risks in cybersecurity for business, government, and society in 2023 • CISO appointed as a Strategic Engagement Advisor to the FBI to further the Bureau's relationship with the private sector

Can’t Stop, Won’t Stop

Optimizing Our Tooling and Processes

We have policies and key metrics established and documented. Security practices are standardized — and incorporated into the overall Equifax business strategy. We’ve reached a stage of our maturity journey where it’s time to focus on optimization.

We’ll fine-tune our tools, data and personnel to extend our fit-for-purpose security aperatus. This will enable us to effectively counter evolving threats and keep ahead of the cyber arms race.

Accelerating Frictionless Security

People will get their jobs done, no matter what. If controls are cumbersome, employees will bypass them (creating risk), make mistakes (creating risk) or accomplish less (and consequently resent security measures). Frictionless security helps reduce risk and improve workforce productivity.

We’ve made meaningful progress embedding self-serve and automation across our business, but we’re not finished. We will refine and scale the capabilities we introduced in 2022, molding every user experience to make it easy for all stakeholders to do the right thing.

Bolstering Identity Security

“Zero Trust” is an overused term. But the principles it espouses — avoiding assumptions, continuously monitoring and leaning into verification — are paramount.

While we’re already enforcing just-in-time and time-bound access for privileged resources, we will leave no stone unturned in our quest to steward consumers’ privacy and minimize attack surface through layered security.

equifax.com