RS/Conference2020

San Francisco | February 24 – 28 | Moscone Center



SESSION ID: CXO-T11

Leaders Needed: Preventing The Next Big Breach



Jamil Farshchi

Chief Information Security Officer, Equifax

- in linkedin.com/in/jamilfarshchi
- @jamilfarshchi



EQUIFAX'S SECURITY TRANSFORMATION



CULTURE

Established a "tone at the top" in support of a security-first culture and built a sustainable team for the future



CONTROLS

Employed a defense-in-depth approach with layered controls designed to prevent or limit the success of an attack



COMPLIANCE

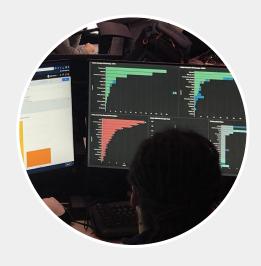
Addressed compliance standards to improve our controls program and strengthen our customer relationships



CUSTOMERS

Partnered with customers and industry organizations to share what we have learned for the collective good





ASSURANCE

Gaining real-time visibility into the assets we have, the controls in place, and how those controls are performing



AUTOMATION

Using standardization, templates, and models to reduce variability and strengthen our ability to remediate weaknesses



AWARENESS

Advancing our ability to share insights and drive effective communication of technical concepts to non-technical partners



ASSURANCE

WE RELY ON DATA, NOT ASSUMPTIONS

This server was left exposed and found by a hacker, who stole the all-important key and used it to access the database snapshot, exfiltrating the information...

InfoSecurity Magazine



The attackers would have been unable to install the malware if [the company] had employed proper network segmentation...

Computerworld



For the second time in two years an SSL/TLS certificate expired and caused downtime...

Hashed Out

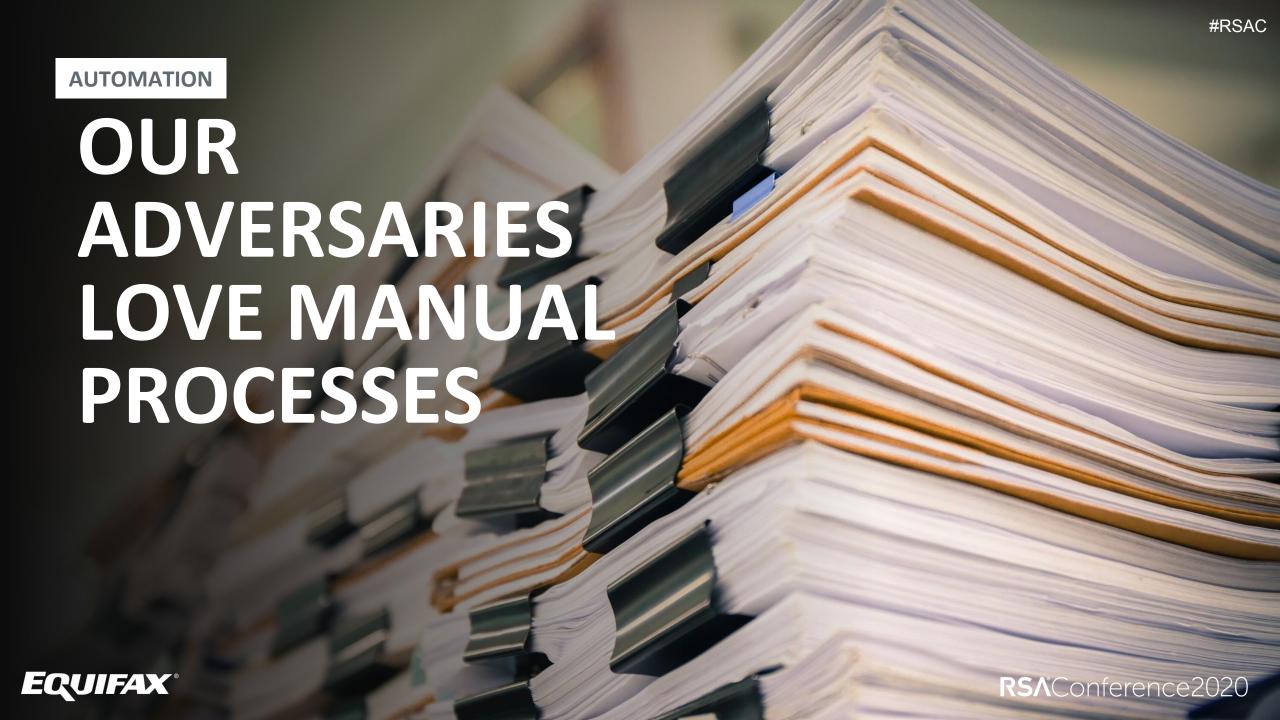


The inaction allowed what's described as "absolutely unsophisticated and uninteresting" malicious code to wreak havoc on the company's reputation...

Harvard Business Review







AWARENESS

CONTROLS PER VECTOR, AND ASSURANCE LEVELS CREDENTIALS NIST CYBERSECURITY NIST PRIVACY FRAMEWORK FRAMEWORK EMAIL / ENDPOINTS DRIVES 1 Asset Management 2 Business Environment 1 24 Inventory and Mapping INSIDERS / 3 Governance POST EXPLOIT A Risk Assessment 26 Risk Assessment 5 Risk Management Strategy 27 Data Proc. Ecosys. Risk Mgmr MATURITY (CMMI) 6 Supply Chain Risk Mgmt. 7 Id. Mgmt. and Access Control BEHAVIOR 8 Awareness and Training 28 Governance Policies, etc. 9 Data Security THIRD PARTY / 29 Risk Mgmt. Strategy 10 Info. Protection Processes 30 Awareness and Training 11 Maintenance 31 Monitoring and Review 12 Protective Technology 13 Anomalies and Events LEVEL OF 14 Sec. Continuous Monitoring 32 Data Processing Policies, etc. ASSURANCE 15 Detection Processes 33 Data Processing Mgmt. 34 Disassociated Processing 16 Response Planning 17 Communications 18 Analysis 36 Data Processing Awareness 19 Mitigation 20 Improvements 37 Data Protection Policies, etc 21 Recovery Planning 22 Improvements EQUIFAX CONFIDENTIALITY, INTEGRITY, AVAILABILITY

