Beware The Coming Data Integrity Crisis

Data Tampering Will Threaten Your Digital Transformation

by Jeff Pollard, Joseph Blankenship, and Trevor Lyness

September 25, 2018

Why Read This Report

Insights-driven businesses are growing at eight times the rate of global GDP and will earn more than $1.8 trillion by 2021. As organizations rush to capitalize on the value of data, security leaders who have historically emphasized data confidentiality will face a new battle over data integrity, where malicious actors tamper with, corrupt, and manipulate the data on which insights-driven businesses depend. This report explains the new investments, capabilities, and roles that security leaders will need so they can give their business colleagues confidence to use and trust the data they collect.

Key Takeaways

Prioritizing Confidentiality Over Integrity Will Soon Expose Firms To Tremendous Risk

Security leaders have tossed the mantle of integrity to business continuity specialists and database administrators. But as businesses adopt data-driven decision making and automation, the lack of attention to data integrity risks could be devastating.

Data Integrity Attacks Will Show Up On Your Risk Register, By Choice Or Not

The Stuxnet virus is one of the best-known examples of an attack on data integrity, the result of geopolitical conflict playing out as cyberwarfare. As such attacks become common among cybercriminals, you will have to address them. Better to start now.

Beware The Coming Data Integrity Crisis

Data Tampering Will Threaten Your Digital Transformation

by Jeff Pollard, Joseph Blankenship, and Trevor Lyness
with Christopher McClean and Elsa Pikulik

September 25, 2018

Table Of Contents

Related Research Documents

The Future Of Cybersecurity And Privacy: Defeat The Data Economy's Demons

The Top Five Emerging Technologies Security Leaders Need To Prepare For

Using AI For Evil

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Data Integrity Matters Now More Than Ever

Forrester has identified a new kind of company: the insights-driven business. This collection of 40 public companies and insights-driven startups will collectively grow at eight times the rate of global GDP and generate more than $1.8 trillion in value by 2021.[1] These companies are the most sophisticated users of data, and as other organizations work to emulate their success, they're using analytics to make important decisions in every department and function. However, this extreme reliance on data to increase the speed of business comes with increased risk:

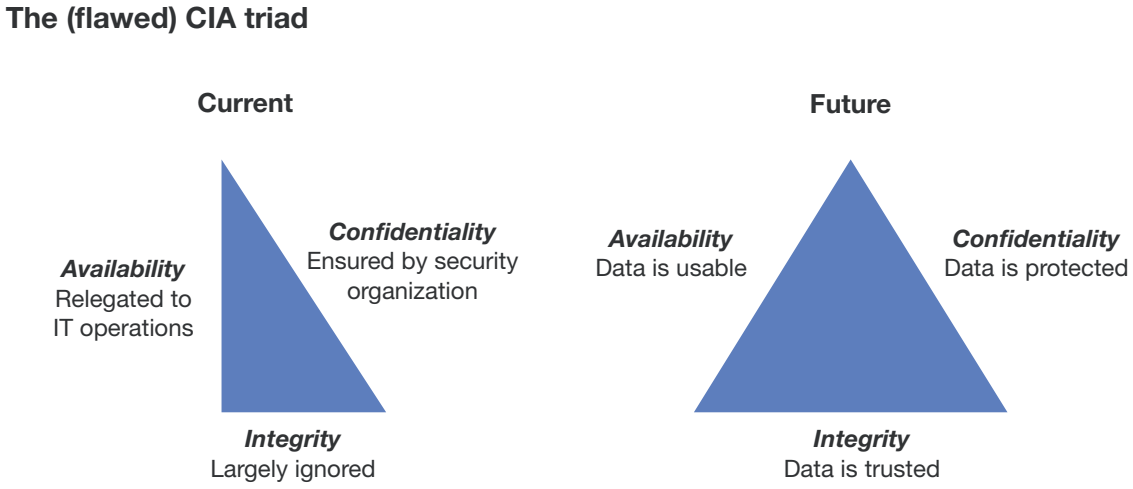
- **Algorithms execute risky actions without human involvement.** Decisions once made by humans, like setting inventory targets, production capacity, and staffing levels, are increasingly made automatically by software.[2] Financial markets are largely driven by trading algorithms that make millions of transactions a day, mostly without human interaction. When these go wrong, they can have broad effects on the markets. The 1987 stock market crash was largely caused by automated trading software preprogrammed to sell at specified prices.[3] Failing to learn from the mistake, the markets in 2010 took another nosedive that was exacerbated by automated software selling off stock.[4]
- **Decisions affecting health and safety increasingly depend on good data.** Modern infrastructure, transportation, and other industrial systems depend heavily on data from sources like GPS satellites and environmental sensors; subtle changes to this data can cause these systems to catastrophically fail. For example, Stuxnet, the cyberweapon designed to derail Iran's nuclear weapons program, changed sensor data from centrifuges, causing them to fail.[5] In 2008, a $1.2 billion B2 stealth bomber crashed as its onboard systems registered incorrect altitude.[6]
- **Fake news and "influence tampering" have real implications.** The amplification of social outrage is a common example of "influence tampering," where malicious actors use fake accounts to multiply a topic's reach on social media. For example, US intelligence officials assert that Russian operatives used social media to sway the opinions and influence the actions of American voters during the 2016 presidential election.[7] In a more direct example, a hacker took over the Associated Press' Twitter feed and wiped out $130 billion in stock value in a matter of minutes with a tweet describing an "explosion" that injured President Barack Obama.
- **Algorithmic decision criteria aren't always clear to humans.** Businesses are using artificial intelligence (AI) and machine learning to automate decisions about everything from financial loans to surgical procedures. Sometimes, the owners of these systems don't know exactly how they reach their conclusions. These "black box" systems can be a risk if businesses can't test the quality and fairness of the input data, calculations, and results.[8] The City of New York passed a bill in 2017 requiring city agencies to learn how algorithms are used to make decisions and if they are biased.[9] The Defense Advanced Research Projects Agency (DARPA) maintains the Explainable AI project that aims to make advances in AI safe.[10]

Attacks Against Data Integrity Will Become More Common

Security pros have long used the confidentiality, integrity, and availability (CIA) triad to describe the foundational objectives of their job function. Confidentiality ensures that information is not accessible to unauthorized individuals; integrity maintains the accuracy of data; and availability ensures that the data is accessible when needed. Availability has and will continue to be a function of IT departments, with some assistance from security. However, security pros focus their efforts too much on confidentiality concerns like threat prevention, breach detection, and sensitive data protection, while paying little to no attention to ensuring data integrity. Specifically, they haven't done enough to make data tamper-proof, tamper-resistant, or tamper-evident. In the future, there will be a more balanced approach to ensure that data is protected against inappropriate access, that data is protected against malicious tampering, and that data is available to the right people at the right time (see Figure 1). Without sufficient attention now, the risks will increase for several reasons:

- **Attackers have increasing incentive to manipulate your data, rather than steal it.** In 2015, former US Director of National Intelligence James Clapper testified that, "In the future . . . we might also see more cyberoperations that will change or manipulate electronic information in order to compromise its integrity."[11] Expect this kind of attack to become prevalent as economic incentives grow. Currently, gaming search engine algorithms or using social media botnets to distort sentiment analysis are two examples of possible, albeit rare, ways that attacks on data integrity can generate a profit. Malicious actors may also use such techniques to demand ransom from their corporate victims, without ever having to send a phishing email, steal credentials, or avoid detection inside a network environment.
- **Insiders can alter data without being detected.** Employees, contractors, and partners have privileged access to systems and data, which means the ability to cause substantial harm.[12] Elon Musk recently announced that an insider at Tesla Motors sabotaged operations by making changes to the company's code base.[13] In the healthcare industry, concern about insiders altering data in clinical trials and putting patients at risk, the British Medicines and Healthcare products Regulatory Agency (MHRA) issued guidance on data integrity, and the US Food and Drug Administration (FDA) is finalizing similar guidance.[14] Furthermore, the Association of Certified Fraud Examiners reported that 31% of fraudsters altered electronic files to conceal evidence of their activities.[15]
- **Manipulation of external data can hurt just as much as internal.** Enterprises get data from numerous external sources to make product, service, and investment decisions. Amazon, for example, makes many of its inventory and pricing decisions automatically, bypassing human involvement.[16] Subtle changes to the data can affect these decisions on a massive scale, exposing enterprises to unforeseen risk. An emerging threat in this area is the proliferation of automated bots, which can artificially inflate demand metrics on websites and cause manufacturers and retailers to believe that a product is extremely popular. If actual consumer interest is tepid, the company could overinvest in product, leading to an expensive failure.

FIGURE 1 Today's Cybersecurity Overwhelmingly Skews Toward Confidentiality



Every Industry Has Unique Data Integrity Risks

Companies and industries are exposed to different data integrity risks depending on how they use data (see Figure 2). Automated manufacturing facilities rely heavily on accurate measurements, and small deviations can cause product defects. In the case of medical device and pharmaceutical manufacturing, patient deaths could occur as a result of poorly manufactured products. Researchers from Politecnico di Milano and Trend Micro demonstrated how attackers could conceivably hack an ABB Robotics IRB140 industrial robot, feed it false configuration data, and cause nearly undetectable manufacturing defects that could lead to catastrophic product failure.[17]

FIGURE 2 Your Use Of Data Determines Your Exposure To Integrity Risks

Industry	Example uses of data	Potential consequences of data tampering
Banking	Evaluate credit worthiness, set service pricing, and block fraudulent transactions.	Issuance of credit to high-risk borrowers; widespread bias; inability to prevent fraud
Healthcare	Use patient records and industry data to diagnose patients and deliver health services.	Poor patient treatment; casualty; medical malpractice suits
Insurance	Price policies and pay claims based on historical and policyholder data.	Widespread mispricing of insurance plans; inability to pay out claims
Manufacturing	Rely on supply chain and testing metrics to manufacture safe, high-quality products.	Malfunction of manufacturing systems or forced recall due to quality or safety issues
Media	Aggregate data from various sources to publish news quickly and accurately.	Publication of fake news, causing reputational and financial damage
Utilities	Modify production and delivery based on usage rates.	Inadequate water, electricity, or gas delivery for municipality, resulting in a public crisis

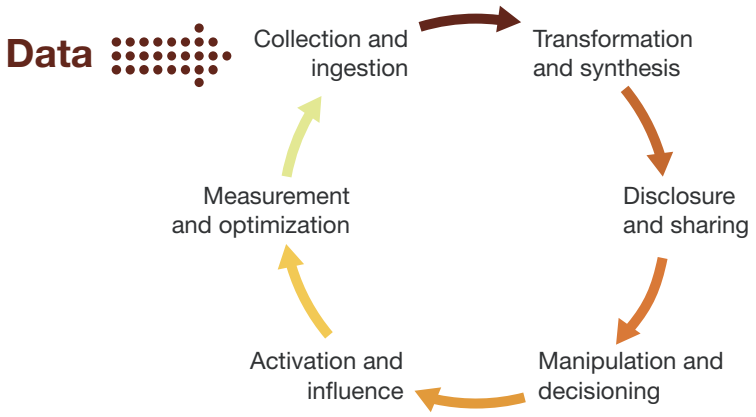
New Threats Will Require New Defenses

Once a business model emerges for attackers, expect these types of attacks to explode in frequency. Black market sites that sell stolen data will add data tampering, for a fee, to their catalog of criminal services; attackers will engage in digital extortion, sabotaging critical data and only providing the original "good" data if a ransom is paid; and cybercriminals will tamper with data to force a company to lose value in the stock market and short the company's stock to turn a profit. Security leaders will have to help their organizations by marshalling in new ways of identifying and managing information risk:

› **Chief information security officers will have to join forces with chief data officers.** In our research, the chief data officers (CDOs) we interviewed were more aware of data tampering risks than the chief information security officers (CISOs) we interviewed. One CDO at a global testing, inspection, and certification company described data integrity as "a core value for us" and attacks on integrity as "a serious business issue." For CDOs, this problem is twofold: First, the information they deliver for insights is trusted by default; second, they risk poisoning customer relationships if they become a supplier of "bad" data, resulting in lost revenue and decreased client satisfaction. CDOs need help identifying, prioritizing, and mitigating risks. That's where CISOs come in.

- **Security programs will need tighter control over data access and manipulation.** Security leaders will need to reassess their current controls to identify which ones can mitigate threats to data integrity in addition to confidentiality. For example, encryption-at-rest is a common control to protect confidentiality, but it's less effective for preserving integrity; if an attacker tampered with internet-of-things (IoT) sensors, encryption would merely ensure that no one could steal the bad data those sensors record. Instead of just locking down data, CISOs will need to enforce controls to monitor data access and modification, sensor modifications, changes to internal data models and algorithms, and anomalies in the decisions coming from these systems.
- **The data life cycle will guide risk mitigation strategies.** For the organization's most important data, security leaders need to know how it can be manipulated during each phase of the data life-cycle path: 1) data collection and ingestion; 2) transformation and synthesis; 3) disclosure and sharing; 4) manipulation and decisioning; 5) activation and influence; and 6) measurement and optimization (see Figure 3). They'll have to work with owners of the most critical processes, products, and functions in the organization and map the supply chain for their critical data. Together, they'll have to design controls for ensuring data integrity across each of the six phases, prioritizing higher risk data with a higher likelihood that an attacker can access and change it.
- **Risk mitigation will have to start with "data endpoints."** Since attacks on integrity can start with individual sources of data — including sensors, wearables, interfaces, and devices — security pros should think of them as "data endpoints." If that endpoint is tampered with, then all data that comes from that source is corrupt. For integrity-based attacks, security leaders will need to think about tamper-proof and tamper-evident solutions for physical hardware in addition to firmware security solutions to offer assurance that the data these devices produce has not been altered or tampered with.
- **Blockchain warrants real consideration for preserving integrity.** While plenty of hype surrounds blockchain, its proofs, ledgers, and traceability have a chance to make a measurable impact as a solution for protecting data integrity. It's early, but technology providers are already building such products. Bureau Veritas is incorporating blockchain in products to improve supply chain data integrity.[18] Future solutions could provide a system of record for data creation and modification in the same way that GitHub and GitLab offer the ability to see check-ins, versioning, tracking changes, and timestamping for source code.

FIGURE 3 Security Leaders Must Ensure Data Integrity Across Each Phase Of The Data Life Cycle



Recommendations

Start Working Now To Take Control Of Emerging Data Integrity Risks

The looming threats against data integrity will receive a spot on your risk register either because you choose to address them or a compelling event will make you wish that you had. Either way, security professionals have time to prepare; incentives for attackers to launch campaigns to damage data integrity are still emerging, so prepare now before data tampering becomes an everyday threat:

- **Conduct an assessment to understand your biggest data integrity risks.** Your organization creates and consumes far too much data for you to ensure the integrity of it all. Start by identifying your business' most important data-dependent processes, such as those that guide customer engagement, service delivery, or financial investments. Next, craft scenarios that simulate how altered data could yield disastrous results. Prioritize the risks that would have the biggest impact on customer loyalty and revenue generation.
- **Recruit a data expert to the security team.** Without a background in statistics and data science, it's tough to imagine the harm an attacker might do by tampering with information, let alone how to detect it. You'll need a data expert to help you understand threat models and attack vectors. We can all imagine the scenario of an attacker gaining access to a critical database and modifying the records within the database; the data expert is there to tell you all the subtle ways the data can be corrupted that might elude more traditional security monitoring.
- **Use bot management tools to fight web-based data tampering.** With most companies interested in strengthening customer loyalty through improved online experiences, malicious bots are rising to the level of archnemesis for data-hungry marketing and customer experience

teams. Bots can pollute web-based analytics such as A/B tests or site traffic, or they may hoard inventory by reserving physical or digital goods in an eCommerce shopping cart. These attacks can lead to inaccurate forecasting, revenue projections, and ultimate success of expensive ventures. Preventing this form of data tampering will require both bot management solutions and advertising verification and brand-safety tools.[19]

› **Adopt digital risk protection tools to prevent influence tampering.** Attackers can target organizations with influence campaigns, designed to spread false information to promote a negative story or damage a brand. Security leaders need to help their marketing and customer insights teams understand the risk that fake news and influence tampering pose to their organizations, track the sources of this information, and work with take-down services to mitigate the risk as much as possible.[20]

What It Means

Technical Advances Will Propel Integrity Losses Past Privacy Losses

Securing confidentiality will seem straightforward compared to preserving the integrity of information, and the complexity and potential damage of integrity attacks are growing with every device we install and process we automate. Computational propaganda already exists and has been used to alter the outcomes of elections, and it can just as easily target your company.[21] Similarly, we've seen comedian Jordan Peele posing credibly as Barack Obama in a fake video, and it's not too hard to imagine fake videos of your corporate spokesperson launching an offensive tirade through various social media channels. Once an attack methodology emerges, it eventually democratizes, and the same will be true of attacks against data integrity. That means cybercriminals intent on disrupting businesses, manipulating economies, extorting your company, or disrupting governments will have far more tools and techniques at hand.

Endnotes

[1] See the Forrester report "Insights-Driven Businesses Set The Pace For Global Growth."

[2] See the Forrester report "The Dawn Of Digital Decisioning."

[3] Source: Stacy Rapacon, "What you can learn from the 1987 stock market crash," MarketWatch, March 13, 2018 (https://www.marketwatch.com/story/what-you-can-learn-from-the-1987-stock-market-crash-2018-03-13).

[4] Source: Alexander Osipovich, "Pentagon Turns to High-Speed Traders to Fortify Markets Against Cyberattack," The Wall Street Journal, October 15, 2017 (https://www.wsj.com/articles/pentagon-turns-to-high-speed-traders-to-fortify-markets-against-cyberattack-1508065202).

[5] See the Forrester report "Protecting Industrial Control Systems And Critical Infrastructure From Attack."

[6] Source: David Noland, "Could One Email Have Stopped a $1.4B Stealth Bomber Crash?" Popular Mechanics, July 2, 2008 (https://www.popularmechanics.com/military/a3414/4271563/).

[7] Source: Molly McKew, "Did Russia Affect The 2016 Election? It's Now Undeniable," Wired, February 16, 2018 (https://www.wired.com/story/did-russia-affect-the-2016-election-its-now-undeniable/).

[8] See the Forrester report "The Ethics Of AI: How To Avoid Harmful Bias And Discrimination."

[9] Source: Lauren Kirchner, "New York City moves to create accountability for algorithms," Ars Technica, December 19, 2017 (https://arstechnica.com/tech-policy/2017/12/new-york-city-moves-to-create-accountability-for-algorithms/).

[10] Source: David Gunning, "Explainable Artificial Intelligence (XAI)," DARPA (https://www.darpa.mil/program/explainable-artificial-intelligence).

[11] Source: Spencer Ackerman, "Newest cyber threat will be data manipulation, US intelligence chief says," The Guardian, September 10, 2015 (https://www.theguardian.com/technology/2015/sep/10/cyber-threat-data-manipulation-us-intelligence-chief).

[12] For more on how insiders can attack your business, see the Forrester report "Defend Your Data As Insiders Monetize Their Access."

[13] Source: Lora Kolodny, "Elon Musk emails employees about 'extensive and damaging sabotage' by employee," CNBC, June 19, 2018 (https://www.cnbc.com/2018/06/18/elon-musk-email-employee-conducted-extensive-and-damaging-sabotage.html).

[14] Source: Mark I. Schwartz, "Agency Publishes Final Guidance on Data Integrity – the British Medicines and Healthcare Products Regulatory Agency that is," FDA Law Blog, April 9, 2018 (http://www.fdalawblog.net/2018/04/agency-publishes-final-guidance-on-data-integrity-the-british-medicines-and-healthcare-products-regulatory-agency-that-is/).

[15] Source: "Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse," ACFE, 2018 (http://www.acfe.com/report-to-the-nations/2018/).

[16] Source: Spencer Soper, "Amazon's Clever Machines Are Moving From the Warehouse to Headquarters," Bloomberg, June 13, 2018 (https://www.bloomberg.com/news/articles/2018-06-13/amazon-s-clever-machines-are-moving-from-the-warehouse-to-headquarters).

[17] Source: Kelly Jackson Higgins, "Researchers Hack Industrial Robot," Dark Reading, May 3, 2017 (https://www.darkreading.com/vulnerabilities---threats/researchers-hack-industrial-robot-/d/d-id/1328790).

[18] Source: "Bureau Veritas Launches Origin, The World's First Blockchain-Based Complete Food Traceability Solution," Bureau Veritas, March 1, 2018 (https://www.bureauveritas.com/home/news/business-news/blockchain-complete-food-traceability-solution).

[19] For more information on bot management tools, see the Forrester report "TechRadar™: Application Security, Q3 2017." For more information on advertising verification and brand safety tools, see the Forrester report "The Forrester Tech Tide™: Adtech For B2C Marketers, Q2 2018."

[20] We identified the 14 most significant digital risk protection providers and analyzed, scored, and ranked them. See the Forrester report "The Forrester New Wave™: Digital Risk Protection, Q3 2018."

[21] Source: "Computational Propaganda," Oxford Internet Institute (https://www.oii.ox.ac.uk/research/projects/computational-propaganda/).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.