Manipulated Data - The Hack You May Not Notice

Hacks, leaks and cyber attacks dominated the news in 2017. However, while these events were generally driven by the hackers intent to gather information either for their own use or for resale on the dark web or for the purposes of extorting money, a more ominous intent may emerge in 2018: data manipulation.

As the *LA Progressive* discussed in a recent article, imagine a major grocery chain getting hacked. However, instead of leaking the company's proprietary information to the public or encrypting its systems with ransomware, the hackers manipulate the data on which the company relies.

What if expiration dates on milk cartons get altered so that some are discarded early while others make drinkers sick, despite appearing within their best before date.

What if figures are manipulated slightly on invoices to vendors, altering the company's balance sheets by hundreds of thousands of dollars.

What if small changes are made to food safety tests so that a product that was failing suddenly looks like it is passing.

Would the company even notice such subtle changes?

Could it still have the confidence that its backups were uncompromised?

How could its investors accurately assess the company's value when all of its financials might suddenly be based on faulty information?

And how might its customers, suppliers and government regulators respond? With legal action?

Now apply this same scenario to banks, medical institutions, critical infrastructure utilities and governmental organizations. The consequences could be catastrophic.

Unlike hacks where data is stolen because it is valuable or hacks where data is encrypted until a ransom is paid to release it, a hack that manipulates data can be very hard to detect, particularly if the change to the vital information occurs in ways that don't attract obvious attention. Moreover, such hacks could also have deadly consequences. A paper in the New England Journal of Medicine, reporting on the risks of data breaches in health care systems, noted that a hacker could, in theory, change a single data point, such as the level of potassium in a patient's blood, leading caregivers to provide incorrect and potentially lethal treatments.

Data manipulation also breeds uncertainty. Where a hacker's goal is to steal information or to encrypt data for ransom, success is dependent on the ability to prove the information is real. But with data manipulation, the goal is to bring uncertainty and in today's data-driven world, the consequences of uncertainty are frightening.

It is not difficult to imagine a data manipulation hack being carried out by a competitor bent on destroying the competition, or by a disgruntled employee determined to destroy his or her employer.

However, while data manipulation hacks may not appear, at least on their face, to be as easily monetizable as say a ransomware attack or the stealing of sensitive data, in the right scenario the hacker could also reap significant financial rewards. For example, an attack could manipulate data in such a way as to call into question the quarterly or annual earnings of a publicly traded company, and having positioned him or herself correctly in the stock market, benefit financially from that attack

A hacker could also "double down" on the ransomware attack by calling into question the validity of the backup data that an organization would otherwise ordinarily use to get itself operational. If a hacker was in the network long enough, the integrity of the backup data could itself be tainted. This could make the organization more amenable to paying the ransom then it otherwise would be.

As data manipulation can undermine the basics of commerce, health, infrastructure and political systems proactive, not reactive, steps need to be taken to address the possibility of data manipulation before this kind of hack becomes more common place.

The first step is to implement basic cyber security hygiene, applicable to all forms of cyber risk. The following is a brief checklist that organizations can use to identify areas that need to be addressed:

- assess your data – what is it, where is it, who has access to it, what controls are currently in place to protect it and what data is the most valuable or critical to the organization;
- identify your risk profile and business goals;
- consider penetration testing your system;
- identify the gaps in your data security, based on best practice or industry standards, and address the gaps, including eliminating the exposure of control systems to external networks and segmenting the network into groups with restricted access;
- guard the perimeter, paying particular attention to any system that connects to the internet;
- ensure that remote access is secure, including limiting the number of accessible applications and using two-step authentication;
- keep current with patches that fix vulnerabilities in computer programs;
- back up data regularly, test backups to ensure they work, segregate from network and store separately, off line and even off site;
- establish policies and procedures governing employees,

management and third party service providers on things such as confidentiality, bringing your own devices to work, password protection, two-step authentication and limited access ;

- educate employees, management and third party service providers through awareness training on things such as data privacy, email scams, phishing attacks, social engineering, secure web browsing, use of unknown devices, etc.;
- establish a cyber security incident response plan, including responsibilities of individuals involved, and test it;

The above checklist is by no means exhaustive and there are many additional points that may need to be considered depending on each organizations industry and business practices. The checklist though can be considered as a high-level guideline to issues that should be addressed regardless of organizational particulars.

In addition, consideration should be given to investing in a system designed to monitor data and carefully watch for data manipulation by regularly comparing live versions of the data to backups. According to 2016 database security industry report in the United States, only 20 percent of organizations surveyed conduct database activity assessments on a more or less continuous basis and 6 percent of organizations never conduct any assessments.

Hacks that result in the exfiltration of an organizations data or that encrypt the data until a ransom is paid can do serious damage to an organization but organizations that are well prepared can often weather the storm. Data manipulation however is more insidious. It undermines not only confidence in the ability of an organization to protect its data but also calls into question the integrity of the organization’s data and therefore all that the organization stands for. Those organizations that down play or worse yet ignore the possibility of their data being manipulated leave themselves vulnerable to legal and regulatory actions, if they survive at all.