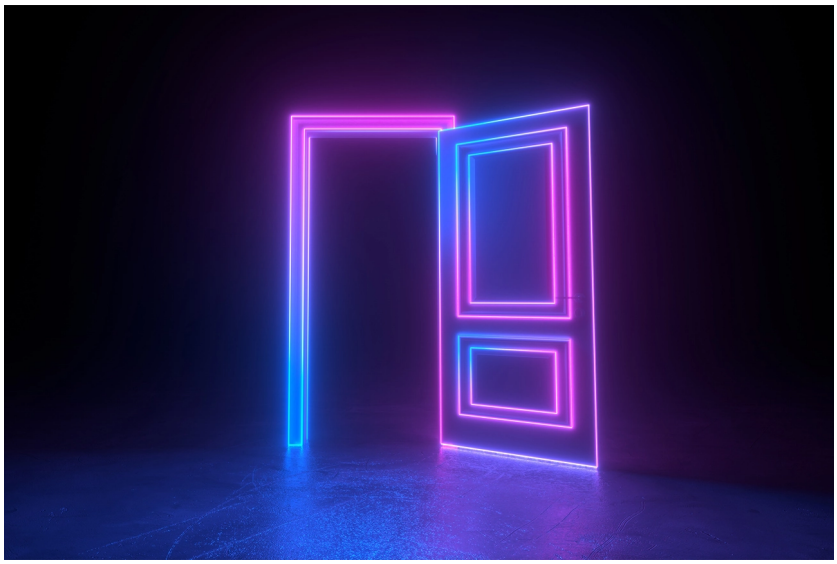
MIT Sloan Management Review

The Rest of the Cybersecurity Story

Semiconscious decision-making is a common but too often unacknowledged cause of cyber risks.

Stuart Madnick • June 21, 2022

READING TIME: 8 MIN



News stories about cyberattacks — SolarWinds, Colonial Pipeline, Capital One, Equifax, and many others — have become all too common. The stories usually focus on *what* happened, with little about the "how" and almost nothing about the "why." But when the "why"

isn't examined, the circumstances that made the cyberattack possible are rarely addressed. What's the rest of the story?[1]

Consider a simple example: A bank is robbed; that's the "what." The "how" might be that the burglar alarm failed to go off. And that's usually the end of the story: There was an unfortunate malfunction.

But digging deeper, we might learn that the alarm system was known to be old and unreliable. Funds had been allocated to replace it, but someone in management decided to instead use them for a marketing campaign to attract more customers.

I call this *semiconscious decision-making*, because someone made a decision — not to replace the burglar alarm — without considering the possible consequences of that choice, namely, losing all the cash. In essence, that decision created the circumstance for the robbery.

That isn't just an interesting hypothetical example; our Cybersecurity at MIT Sloan (CAMS) research group studied many cyberattacks and found that every major attack was a result of semiconscious decision-making, which is rarely studied and thus rarely corrected.

Multiple Layers of Defense

There's an adage that thieves have an advantage because they only have to find one way in, whereas the

defenders must be sure that every entryway is locked. But actually, defenders often have the advantage.

In the case of a cyberattack, this is because the attacker must successfully complete multiple steps, each of which offers the defender an opportunity to halt the intrusion or at least mitigate its impact. Effectively, the attacker must find not simply a single way in but the precise sequence of steps that will enable the cyberattack to succeed.

What's the rest of the story behind our bank robbery example? It might not be reported that the bank president had given the vault lock code to an assistant, written on a piece of paper left atop the assistant's desk, which the burglars were able to find. Further, the security cameras, reasonably expected to record the event (and likely enabling identification of the burglars), were still programmed with the manufacturer's default security password, which the attackers used to disable the cameras and erase any recorded video. All of these gaps must have been overlooked by the defenders and found by the attackers.

This bank robbery might sound like a far-fetched example, but most major cyberattacks do indeed exploit multiple flaws in an organization's defenses, as the CAMS research team has uncovered. One of the most popular descriptions of typical cyberattacks is the Mitre ATT&CK framework, which identifies up to 14 steps that attackers need to take to steal information. Getting into the target's computer systems is only an early step of a

successful data breach. Much more work must be done to find the valuable data and move it to the attacker's computer, referred to as *data exfiltration*, and all of this must be done without the victim noticing.

The CAMS team has developed the Cybersafety methodology and has applied it to analyze multiple cyberattacks (as well as to prevent cyberattacks), including the 2017 Equifax breach. (See "The Equifax Hierarchical Control Structure" figure.) The methodology is based on three core concepts: (1) Identify the crown jewels — that is, what is it that you are trying to protect or prevent; (2) identify controllers for processes that are intended to protect the crown jewels; and (3) identify controllers for controllers, hierarchically. In essence, an attack can only succeed if the needed controls were defective or simply not in place — and if a higher-level controller overlooked this security gap.

The Equifax Hierarchical Control Structure

The Equifax system had 19 unique safety control loops spanning four levels of the safety control structure, each a potentially insecure entry point.

DOWNLOAD THE FIGURE

Semiconscious Decision-Making in Practice: The Rest of the Equifax Story

Consider the case of Equifax, whose hacked data exposed the personal information — including names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers — of 148 million people. As reported in the press, the attack sounded like a simple, isolated accident: "According to Equifax, the breach occurred when 'criminals exploited a U.S. website application vulnerability to gain access to certain files.'" Assuming that the problem was quickly fixed, there should have been nothing more to worry about ... right?

Applying the Cybersafety methodology in order to reveal the what, how, and why of the cyber event, we identified many cases of semiconscious decision-making that contributed to the Equifax data breach. These semiconscious decisions were made at all levels of the organization, from the middle management of technical groups to top executives and the board. Let's consider just two of those decisions.

Unencrypted Data

Equifax used almost none of the basic practices considered good cybersecurity hygiene to protect its

systems and data. One of the simplest and most important defenses against a data breach is to encrypt data so that even if the data is exfiltrated, it remains useless to the attacker.

But much of the data stolen from Equifax was not encrypted. The press reported that the company's Automated Consumer Interview System (ACIS) website had the vulnerability and was the entry point for the cyberattack. But ACIS, categorically, *should be* subject to the Payment Card Industry Data Security Standard (PCI DSS) for protecting credit card holders' data, which requires that all data be encrypted. Furthermore, such systems are usually subject to annual audits to ensure that all the PCI DSS requirements are met.

Equifax management had decided to purposely exclude ACIS from the PCI DSS audit. In retrospect, ACIS likely would have failed most of the 12 PCI DSS requirement categories — including the need for all data to be encrypted. Despite knowing that ACIS should be subject to PCI DSS requirements, decision makers at Equifax didn't make compliance a priority — at the cost of over $1 billion.

Outdated Certifications

Second, the company's intrusion detection and prevention process (IDPP), which was supposed to be monitoring internet traffic for any messages that were suspicious or invalid, had not been functioning *for at*

least nine months. Only when it was fixed was the ongoing cyberattack discovered.

Why wasn't the IDPP functioning? It required certain security certificates to give it permission to access the internet traffic, but the certificates had expired — so it was not able to monitor any traffic or sound an alarm.

Why hadn't the certificates been updated long ago? Well, Equifax had hundreds, if not thousands, of such certificates, and tracking each one's expiration date and updating the certificates was an error-prone, manual task (not unlike the defective burglar alarm process in the bank robbery example). This problem had been noted in the past; in fact, a proposal had been made to develop an automated, centralized certificate-management process. But the managers responsible for the numerous applications requiring security certificates, scattered throughout the organization, did not consider this a priority. Furthermore, providing centralized support for managing the certificates would require some organizational changes that were likely to be resisted by those who had overlooked the danger created by expired certificates.

Conscious Risk Assessment

Apparently, no one at Equifax considered the possibility that these two isolated decisions, along with many other

similar semiconscious management decisions, might cost the company dearly. The company's board essentially allowed management to take unmeasured, and thereby unlimited, risks in order to pursue an aggressive growth strategy. Although all of Equifax's board members had considerable experience in areas such as executive leadership and strategy development, only two of the 10 had any expertise in cybersecurity, according to company reports. (We found this to be a common element at the top of most of the organizations we studied.)

It is fine for management to have a "risk appetite," but when it comes to cybersecurity, the risk potential must be consciously and realistically evaluated. Most attacks that we studied stemmed from decisions made without any explicit consideration of risk. The connections between decisions that might seem minor and the significant consequences those decisions can invite are rarely considered.

While some risks are true surprises unlikely to be recognized in advance, many are more like the burglar alarm known to be defective. Indeed, in almost every case that we studied there were red flags — often many of them — that management chose to ignore, with disastrous consequences.

Organizations are familiar with assessing traditional risks, such as when deciding where to build a new plant or dealing with currency fluctuations. But risks related to cybersecurity are new to most organizations; the

connections between what are seemingly minor decisions and the consequences of those decisions are seldom part of their past practices or experience.

Leaders can do at least two things to improve this situation. First, management at every level must gain knowledge about how cyber risks arise and hone their skills in assessing the potential consequences of breaches. Reading detailed analyses of past cyberattacks, such as those at Equifax and Capital One, and participating in tabletop exercises and cyber fire drills, are a couple of ways to accomplish this. Second, when managers at all levels are developing plans to improve revenues or reduce costs, they must consciously and deliberately assess the potential cyber risk of the planned changes — and then, only if the risk is acceptable, proceed. Taking these steps can dramatically reduce the number of cyberattacks your company faces while minimizing the impact of any attacks that do successfully breach your systems.

Topics

Managing Technology | IT Governance & Leadership | Security & Privacy

ABOUT THE AUTHOR

Stuart Madnick is the John Norris Maguire Professor of Information Technologies, Emeritus, at the MIT Sloan School of Management and the founding director of the Cybersecurity at MIT Sloan research consortium.

REFERENCES

1. "The Rest of the Story" was a radio segment that aired for more than 30 years, ending in 2009. In each episode, host Paul Harvey presented the backstories of historical events and always ended his broadcasts with the tagline "And now you know the rest of the story."

TAGS: Cybersecurity, Data Management, IT Governance

REPRINT #: 64107