DATA Integrity

For most of my career, data integrity was largely a technical matter that IT folk talked about when building and securing databases. It, with process integrity, is vital. Increasingly, data integrity is becoming everyday parlance, a term and topic with growing reach and relevance.

Take the Bodleian Library in Oxford, for instance, which was founded in 1602 and is famous as a setting for the library scenes in Harry Potter. I was hosting a US Cabinet member at the library and our fairly traditional-looking guide talked us through the challenge of holding a copy of every book published in the UK. They'd considered digitization, but problems with "data integrity" meant that the digital versions could not replace the hard copies. Those copies still had to be stored—at considerable expense—even though most were never looked at. The printed page, it seems, has more integrity than data on a server.

"Work on the assumption of compromise, either technical or human," advises Brunswick's **PADDY McGUINNESS.** "Be prepared and expectant without being fearful."

Then there was Cyprus, a country close to the conflict in Syria. A Syrian air-defense missile recently missed its target and fell on a Cypriot mountain side, bringing the battle close to home. A Cypriot government official told me of the increasing concern at the loss of reliability from GPS data in Cyprus's sea area and airspace. It seems that the Russians (and thus the Syrians) distort GPS data to impede reconnaissance and complicate or even prevent targeting by Western weapon systems. The effect can be felt in the positioning, navigation and timing systems integral to so many transport, communications and industrial systems. The official told me "data integrity" had been lost.

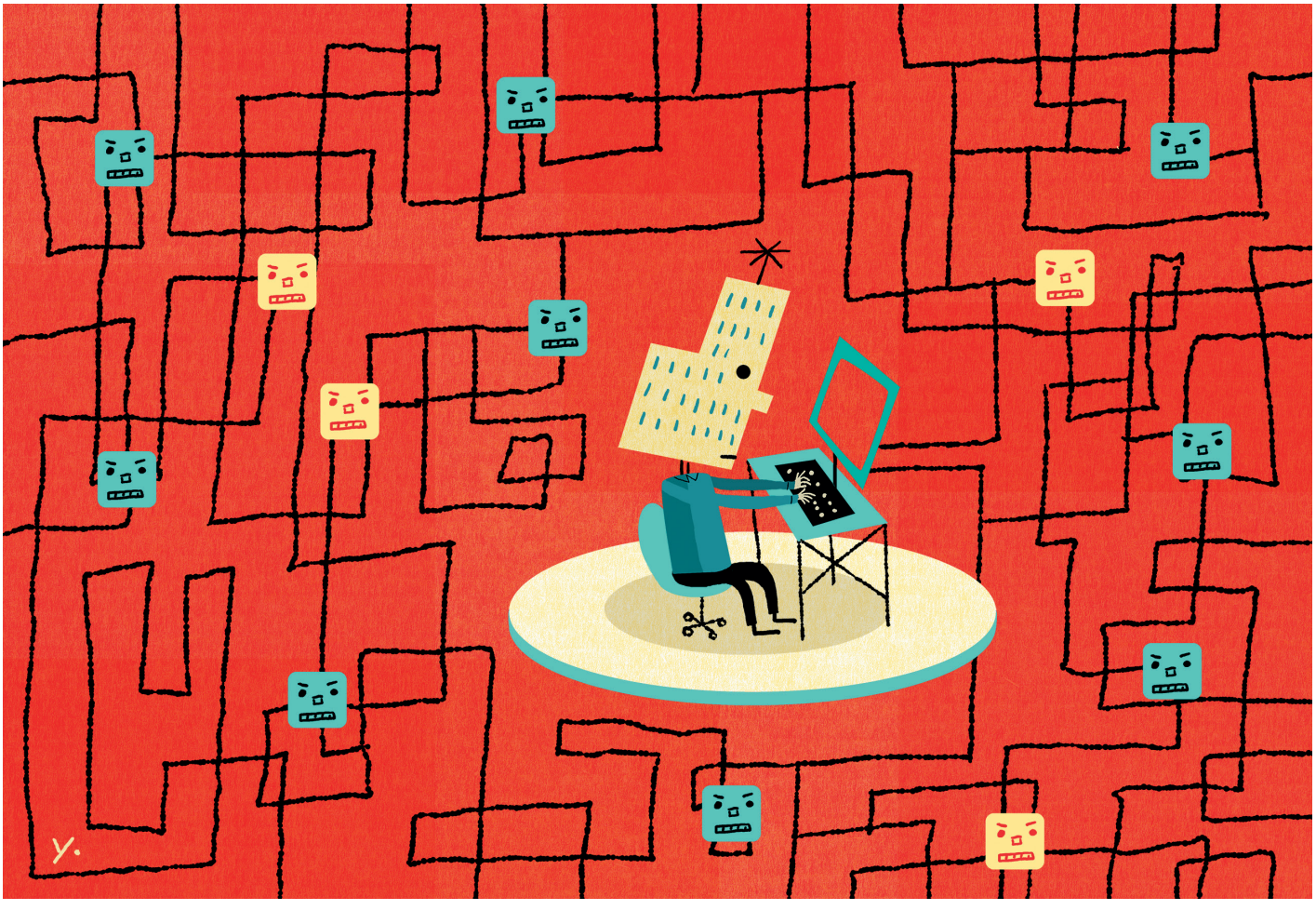

ILLUSTRATION: JAMES YANG

It's a stretch to describe computational propaganda or "Fake News" as a data integrity issue—that presupposes the other "innocent" data we receive, curated via news outlets or social media, has integrity.

There are already plenty of well-known online threats to data integrity, such as links that take us to pages that appear to be from a trusted provider (your bank) but are actually fake. While other online threats are only starting to surface. We are still learning how to manage "deepfakes," audio or video content that has been so convincingly altered it's difficult to tell it's inauthentic.

The vulnerability is yet greater if the telephone networks that we connect to are not themselves secure. Imagine the surprise in Iran when users accessing web pages through 3,500 switches found that, instead of receiving the results of their search, they saw a fluttering Stars and Stripes and the message, "Hands off our elections." This is the network vulnerability companies and governments are trying to prevent when they talk about network equipment not yet being resilient. This was a pretty clumsy attack. Consider what the effect would have been if the attacker, rather than replacing the whole searched-for page, had altered one or two items in a trusted news source, say the BBC or Reuters, to publish their article on your phone.

Many of these emerging threats to data integrity touch global organizations, which is why the term has made its way to the boardroom.

A client recently asked me what I thought of the "integrity" of the data on which their board are basing their data and cyber resilience decisions. Like so many executive committees or boards, they have a "data and cyber" agenda item at every meeting and have plenty of reporting on performance against controls and emerging risks. They have RAG-rated (red-amber-green) charts that non-executives dissect, complaining that the risk and mitigation data is presented differently for the other boards on which they sit. There are occasional blood-chilling briefings on threats from former national security officials like myself, or sessions where executives recount what it was like enduring a catastrophic cyber event.

My client complained that while they knew what was happening on their networks, they didn't really know what was happening elsewhere. They had bought threat intelligence services that scrub the darknet looking for compromised data. They had signed up for government- and industry-run information-sharing partnerships in the jurisdictions where they operate. But still they felt uneasy about what they didn't know.

"While they knew what was happening on their networks, they didn't really know what was happening elsewhere ... they felt uneasy... As they should: The position is likely worse than they understand."

As they should: The position is likely worse than they understand. What they know is what their existing controls illuminate—what might be termed the "known ambient threat." The chance of those controls being ahead of emerging threats and malicious insiders is quite small. Board members typically look for external tests of their internal controls, and cite what happened in company X or what security service provider Y is saying. They are especially influenced by public reporting of major data and cyber events (and the increasingly large regulatory fines).

But this approach falls short; not all incidents are reported or become public. A quick scrub of the many major cyber incidents that Brunswick has handled for clients this year reveals that in the UK and Europe, fewer than 50 percent voluntarily went public with the breach, while 60 percent ended up being made public. In the US, roughly 30 percent wanted to go public but 80 percent became public eventually.

In the UK and Europe, around 75 percent of clients had to report the incident to some regulatory body, while roughly a third claimed against insurance policies. In the US, roughly 60 percent reported to a regulator (including state attorney generals), and more than 80 percent claimed against insurance policies. In other words, the picture painted by regulators, the media and insurers is incomplete.

Even when an incident becomes public, the full nature of what happens is rarely revealed, either because of investigatory or legal constraints or simple corporate diffidence. This may change if mandatory breach reporting is required by law or if cross-sectoral data sharing at machine speed becomes standard—but that's nowhere near the case today.

And notice the strikingly different insurance claim figures between the US and Europe. The European market is less developed, with the consequence that there are too few claims in Europe for there to be a reliable actuarial risk model. We just don't know how great the risk is.

Where does this leave my client? My advice was to work on the assumption of compromise, either technical or human, and build up organizational resilience against the potential fallout—to be prepared and expectant without being fearful. This gap between the reality of the cyber risk and what is planned for will close eventually, just not any time soon. ◆

PADDY McGUINNESS is a Senior Advisor with Brunswick. He was the UK's Deputy National Security Adviser for Intelligence, Security and Resilience where he advised the Prime Minister and National Security Council on policy and decision-making on homeland security issues, leading on the UK's cyber strategy and programs.

Enter the IMPOSTOR

Disinformation attacks pose a growing threat that investors and corporations may not be prepared to handle. Brunswick Insight's **ROBERT MORAN, PRESTON GOLSON** and **ANTONIO ORTOLANI** lay out the results of their recent research.

BUSINESS AND INVESTORS RELY ON INFORMATION, the integrity of which is essential to profitable investments. Parsing truth from error has always been a hazard. Now, however, disinformation attacks on corporations have become a game-changer to be factored into market valuation strategies. False information can be spread digitally with the aim of damaging corporate reputations and investor confidence. Emerging "deepfake" technologies can make realistic recordings that portray executives saying things they did not.

Brunswick Insight research suggests investors are waking up to the ramifications digital disinformation will have on the ability to distinguish between real and fake. In a survey of US investors with over $250,000 in investible assets, 88 percent of investors consider disinformation attacks on corporations a serious issue.

More than two-thirds think corporate disinformation will become more common in the next few years. The actors they are most concerned about are financial fraudsters, followed by hostile foreign governments. Businesses with interests tied closely to competitive geopolitical matters may find themselves in the crosshairs of a hostile nation-state seeking to use any means to disadvantage an American company. Almost two-thirds of investors surveyed thought it would be difficult to tell if a negative story or post spread by a foreign government was true.

Investors pointed to false information surrounding M&A announcements and IPOs as potentially the most damaging. The personal conduct of an executive or stories suggesting a product is unsafe are other likely and vulnerable targets. Imagine the effect of a doctored video slurring the words of an executive to make it appear they have a health issue on an earnings day or amid succession speculation.

Almost 60 percent of those surveyed were not confident other investors could distinguish between real news and disinformation. Barely over half were confident they could themselves. Adding to those concerns, only 17 percent of investors surveyed had even heard of deepfakes. With such limited knowledge, they are understandably split on how big a concern deepfakes really are. When a malicious actor puts out a video spoofing a statement from a CEO—will investors even know the video might not be real?

For executives, the survey data offers important clues for how to proceed. Following a negative report, over 70 percent of respondents said they would look at the company's official communication channels to establish factual information. This means companies need to have well-established and authenticated channels where that information could reside.

The investor data also raises key questions for executives. Have companies prepared for disinformation scenarios so they have established practices for quickly relaying facts and enacting communication protocols that integrate the CEO, corporate communications, investor relations and their legal teams? Do they have effective social media monitoring and early warning systems? Do they have their own authenticated video of a key statement or event to guard as insurance against imposters?

The goal of disinformation is not just to deceive, it is to annihilate the truth and get the public to question reality itself. The effect of corporate disinformation on markets can be toxic.

The sooner companies and investors face up to the reality of these new challenges the better. ◆

ROBERT MORAN is a Partner in Washington, DC, and Head of Brunswick Insight, the firm's public opinion, market research and analytics arm. **PRESTON GOLSON,** in Washington, DC, is a Director and a former CIA spokesperson. **ANTONIO ORTOLANI,** in New York, is a Director specializing in global media analytics.

ILLUSTRATION: JAMES YANG

Manufactured MOB

Zignal Labs CEO **JOSH GINSBERG** offers Brunswick's **PRESTON GOLSON** and **ANTONIO ORTOLANI** his insights into disinformation attacks and what business can do to combat them.

HEIGHTENED SOCIETAL DIVISIONS ARE OFTEN played out and worsened on social media. In this environment, bad actors run influence operations to manufacture sentiment and manipulate public conversation and opinion.

Malicious actors often hijack conversations across the entire media spectrum with the help of automated disinformation networks. These networks sow division and stoke the combustible tinder of online controversies that then filter into the real world. Increasingly, these tactics are being turned against businesses in ways that affect their bottom line.

Zignal Labs—a full-spectrum, real-time and predictive media analysis company—makes it its business to understand the threat that influence operations and disinformation pose to corporations. Its CEO Josh Ginsberg and his team have found that virtually any Fortune 1000 company could be a victim. Worse, by the time a company is aware of a carefully coordinated attack, a wildfire of false information may have already spread to the real world.

Mr. Ginsberg groups the direction these disinformation attacks can take into three categories.

News amplification to fuel controversies: High-profile cultural debates are prime targets for influence operations, says Mr. Ginsberg, who spent years running political campaigns. Influence operatives can deploy coordinated disinformation networks to play up both sides of an argument and drive controversy.

"By subtly influencing the direction and amplification of real discussions and controversies, disinformation can make these stories sound bigger than they are, turning up the volume on our already polarized climate," he says. "If disinformation can amplify, say, a controversial statement by a celebrity, imagine what it can do around a business controversy."

Reputation attacks against a brand: Traditionally, a crisis surfaces in several negative news cycles, before the media eventually moves on to other stories. But today, using social media, disinformation networks can put a company's failures on repeat for months or even years on end, recycling and amplifying old news to alter public opinion around a brand.

Assaults to impact stock price: Corporate reputation is often tied to the value of its shares, making earnings reports and other company statements particularly vulnerable occasions. "We've seen instances where automated networks amplified and elevated an unverified cybersecurity report by an obscure source over a period of days in order to affect the stock price," Mr. Ginsberg says.

SO WHAT CAN BE DONE?

"Companies need digital safeguards," Mr. Ginsberg says. This includes solutions that monitor, detect and then notify of coordinated manufactured sentiment online so companies have the opportunity to determine they are under a disinformation and misinformation attack. "With this warning, teams can plan their communications response strategies and counter with proactive messaging or a public denouncement of the false activity," he says.

Heightened awareness of the threat allows companies to forecast the potential time and nature of manufactured sentiment, as well as do their homework on the tactics and networks being used. Companies can better target how they may be able to best intervene to mitigate the spread of false information.

Methods to push back against the manufactured mob are in the early stages of development. But it is clear that having the means to both spot attacks and to quantify the threat early can help businesses best assess the nature of the threat and decide on the most appropriate course of action. ◆

ANTONIO ORTOLANI is with Brunswick Insight in New York. **PRESTON GOLSON** is a Director in Washington, DC.

ILLUSTRATION: JAMES YANG