My Account Cards Travel Rewards Business Log In

DON'T do business WITHOUT IT℠

Trends and Insights > Getting Customers

Search Trends and Insights

December 08, 2018

Risk Management 101: How to Help Protect Your Company From Fraud

Digital transformation has ushered in new risk-management challenges, and protecting a business from fraud is more complex than ever. From data security to third-party risk, the interconnected digital ecosystem requires businesses to adopt new risk-management solutions.

Rodika Tollefson
Freelance writer and journalist

Fraud prevention is daunting: In a 2017 survey by Experian, 72 percent of 500 businesses in 11 countries cited fraud as a growing concern over the past 12 months; 63 percent of businesses have experienced the same or more fraud losses in the last 12 months.

Data breaches is one trend impacting risk management. Every second, 72 data records are lost or stolen, estimates digital-security company Gemalto's Breach Level Index, which tracks publicly disclosed data breaches since 2013. The database shows nearly 13.5 billion records were compromised in the last five years—and data-security professionals say this translates into financial risk for businesses.

"The reality of our current times is that data is money," says Brian Golumbeck, executive director of risk transformation at Optiv Security.

Golumbeck says that while organizations take steps for financial-risk management, many lack in "protecting data that can hold great value."

"Simply put, data risk is financial risk and companies need to take information security as seriously as they take protecting financial assets," he says.

Stolen Identities and Credentials

Based on a 2017 survey of 800 fraud-mitigation professionals across six industries, LexisNexis Risk Solutions found that fraud from stolen identities or cyberattacks was of greatest concern. More than three-quarters of respondents said they used external data and analytics to mitigate fraud, including behavioral analytics and predictive modeling.

“Data analytics can be very effective in detecting and preventing cybercrime,” says attorney and certified fraud examiner Ron Cresswell, a research specialist with the Association of Certified Fraud Examiners (ACFE).

Fake accounts now look more authentic, says Kevin Lee, trust and safety architect with Sift Science, which provides a digital trust platform.

“Because there's so much access to identity data from various data breaches or from people sharing online, fraudsters are creating some very good accounts,” he says.

Lee previously led trust and safety teams at Facebook, Square and Google, and has seen the number of so-called synthetic identities and accounts grow. He says in the past, businesses faced simpler schemes like stolen credit cards, but that's changed.

“Now, based on the richness of data that’s out there, fraudsters are able to piece together your identity, and it puts fraud fighters in a difficult bind,” he says.

That’s where data analytics comes in.

“It's becoming easier and easier to mimic a user, so user behavior is a big differentiator,” Lee says.

Businesses should monitor the dark web for user data, says Christian Lees, chief information security officer at identity-protection company InfoArmor (recently acquired by Allstate Corp.). Another organization’s data breach or compromised user credentials could impact your business, he says.

“We often tend to reuse username and passwords across a number of sites, and sometimes people use corporate credentials for these third-party sites,” Lees says.

Third-Party Risks

Fraudsters use stolen credentials to pose as trusted parties such as vendors. Yet many businesses don't realize the risk from their real-time interconnected ecosystem, says Fred Kneip, CEO of CyberGRX, which provides third-party risk protection.

“Third parties create trusted connections… and if you come in under the guise of a third party that's trusted and has access, it's a lot easier,” says Kneip.

He says that the access businesses give partners increases the attack surface for fraud perpetrators—but there are effective prevention strategies. One is to conduct a risk assessment and audit to understand “what your landscape looks like.”

Other strategies that could eliminate opportunistic attacks, he says, are software patching and phishing awareness training.

“The vast majority of exploits take advantage of software that can be patched,” he says. “Second, the vast majority of breaches originate with a phish—an email with a (malicious) attachment or link.”

Phishing Scams

Tammy Martin, founder and CEO of CFO Strategic Advisors, which provides fractional CFO services, has watched phishing schemes evolve. One scam her firm regularly encounters is business email compromise (BEC), which typically involves phishing to take over a legitimate email account and conduct unauthorized fund transfers or steal employee data.

The FBI has seen a 136 percent increase in identified global losses from BEC between December 2016 and May 2018, and says the total loss since 2013 is $12.5 billion.

> “
>
> Simply put, data risk is financial risk and companies need to take information security as seriously as they take protecting financial assets.
>
> *–Brian Golumbeck, executive director of risk transformation, Optiv Security*

One example of how fraudsters are changing their BEC schemes, Martin says, is the common, urgent request to purchase gift cards for clients.

“Once these gift cards are emailed to the scammer, these funds cannot be recovered,” she says. “In my experience, many businesses are focused on $30 gas and $50 meals charged to business credit cards, but not focused on bigger external threats like $4,700 worth of gift cards that just went out the door.”

Human resources, finance and accounting departments are phishing targets because they have access to valuable data. Martin believes their training should be customized, yet many businesses instead “roll out a generic, one-size-fits-all training approach.”

Internal Fraud

Internal, or occupational, fraud resulted in more than $7 billion total global losses to businesses in 2017, ACFE found. According to ACFE's 2018 Report to the Nations, based on the results of the 2017 Global Fraud Survey (based on 2,690 cases of occupational fraud), fraud lasting more than 60 months is more than 20 times as costly as fraud detected within six months.

"You want to catch fraud as soon as possible," Cresswell says.

ACFE found that internal control weaknesses were responsible for almost half of fraud incidents globally. While data monitoring and analysis resulted in 52 percent lower losses and 58 percent faster detection, only 37 percent of victim organizations used these tools.

Code of conduct and external audits of financial statements are the most-common anti-fraud controls in the United States, according to ACFE. Cresswell also recommends checks and balances such as separation of duties for certain financial tasks (e.g. payment approval and writing checks), job rotation and mandatory vacations.

"Many frauds are discovered when the employee perpetrating the fraud is out of the office," he says.

Additionally, Martin suggests taking advantage of tools available from financial institutions. Some corporate credit cards allow business owners or managers to monitor and control their employees' spending by predefining spending limits, restricting cash advances and creating flexible expiration dates and other flexible spend controls. For example, she advises keeping the spending limit low and increasing it temporarily when the employee is traveling on business—and notes that some credit card companies can even send the owner or manager a text alert when the limit is exceeded.

"Having the right credit card partner will not only help businesses have stronger fraud controls, but they can often earn points and even rebates from these card companies that allows them to lower their overall costs," Martin says.

"Businesses must use a targeted approach to preventing fraud by implementing continuous training, leveraging technology and insuring against fraud where appropriate," she says. "This has to be ongoing—and is usually the area where businesses need to spend more time and effort."

Photo: Getty Images

Want to Dig Deeper?

Digital Tools | Rodika Tollefson | Getting Customers

About the Author

Rodika Tollefson

Freelance writer and journalist