INSIDE BUSINESS
FOCUS ON CORPORATE SECURITY AND DISASTER PREPAREDNESS
AUGUST 2, 2019 · www.CPBJ.com

Vijay Varadarajan
...We're trying to bring the manufacturers and technology together and have them develop a cybersecurity plan...
Page 11

Next week: Top 250 private companies

DOUBLE-EDGED SWORD

Digital technology can help businesses – except when it doesn't

By Martin Daks
Contributing writer

A pair of chainwide cash register crashes at Target Corp. in June, right around the heavy-sales Father's Day weekend, may have cost the national retailer $50 million to $100 million in lost sales, according to some analysts.

The problems — one of which the company blamed on a "technology glitch," while another was traced to a tech center run by NCR Corp. — were quickly corrected, but they also point to a deeper issue, said some local experts: Technology has helped to boost business productivity, but it's also exposed companies to a host of challenges.

Stoneberg

"There is indeed a tradeoff between absolute security and meeting business needs and functions," said Richard Stoneberg, chief information security officer of Allentown-based Netizen Corp., which serves as a 'virtual' CISO for several businesses. "If I turn off my computer, put it in a vault and I am the only possible person who could open it – I truly have very good security on that computer. But it is not terribly functional for me either. So the suggestion is pretty straightforward: Do a true IT security overview of your data and processes in a risk-based, cost-effective mindset."

Each business will have a unique solution, he added, and "even businesses in the same type of work can be different. There are cloud-based solutions that can work," as well as redundancies and others that can reduce the risk of outages.

In general, there are three "pillars of good security," according to Stoneberg: confidentiality, integrity and availability. The first involves considering how data is kept confidential or secured against hackers. Integrity refers to the correct billing or charge to the correct person at the correct time, while availability ensures that a customer can actually purchase a company's goods.

Preserve human element

The human component is another important factor, according to Devin J. Chwastyk, a Harrisburg-based member of McNees Wallace & Nurick LLC, and chair of the law firm's privacy and data security group.

please see TECHNOLOGY page 10

For employers, words of warning on FaceApp

By Brian Pedersen
BridgeTower Media

FaceApp has seen a surge in popularity and, with it, notes of caution.

The free mobile app allows users to take selfies that are then transformed by artificial intelligence to look older, add features or even change genders.

But while the app may be fun, some observers note that the technology raises privacy concerns, particularly for employers with bring your own device policies, known as BYOD.

A company's data could be compromised if employees download the app to devices they use for work.

That's because the app gives its developers access to whatever else is on a device, including other data stored on it, said Doug Panzer, a patent attorney for Fitzpatrick Lenz & Bubba, based in Upper Saucon Township.

The maker of FaceApp is a Russian company, Wireless Lab OOO of St. Petersburg.

"We cannot know for certain the uses that the FaceApp developer will make of the information it collects since we do not have firsthand knowledge of the internal operations of the company," said Panzer, who said he has downloaded and used the app and read the terms of service and privacy policy.

The terms note the company can send data to other partners, including other companies in the same legal group as Wireless Lab, Panzer said.

Panzer said the terms also give far-reaching rights to Wireless Lab over the use of the photos that users provide to and create with the app. In addition, the terms give the company access to significant technical data that the app may collect or even store on a person's device, he added.

Even if you delete the app from a mobile device, it may not delete all of the data, he said.

One potential solution is a factory reset of the phone, but again, it may not be a sure fix.

For employers, a dose of prevention could help.

Employers with BYOD policies should rely on management tools that control what employees can – and cannot – download on their devices, said Michael Hawkins, founder and CEO of Netizen Corp., a cyber security company in South Whitehall Township.

Hawkins said he has seen people using FaceApp all over Facebook.

"While it may not currently be nefarious, with the information they are collecting, it could be used against you at some point," Hawkins said.

The biggest concern for Hawkins involves government employees or others with access to sensitive data through their work phones.

The information is going to a U.S.-based server but then goes to the Russia-based company, he added.

"Nobody reads the terms of service," Hawkins said. "This is the perfect example of what they call a honey trap." ■

TECHNOLOGY

continued from page 9


Chwastyk

"Keep in mind that the vast majority of computer crime and hacking incidents are usually traced to security and other vulnerabilities associated with the people using a computer," he noted. "It's a matter of HR training so employees will avoid clicking on unknown links and engaging other risky online behavior."

He said some regulated industries, such as medical facilities that are governed by HIPAA, or the Health Insurance Portability and Accountability Act of 1996, have been "ahead of the curve when it comes to training, controls and best practices, but now they're trickling down to other industries."

Chwastyk also had advice for companies that tie their IT systems to vendors' setups. "We work on these kinds of issues and address them with contractual terms," he said. "You want terms in the agreement with vendors to define issues like the level of performance to be delivered, and what kinds of remedies will be available if they fail to meet those standards."

Businesses may also wish to consider cybersecurity and business interruption insurance policies, he added.

"Depending on the circumstances of an incident, there may also be reporting requirements," he noted. "Generally, a simple outage won't trigger them, but all 50 states have notification requirements for a ransomware or other security breach that exposes personally identifiable information. If your company does business internationally, you may have to consider European Union and other reporting requirements."

Cost matters, too

Companies need to ask themselves "what's it worth to me to keep my operations up and running?" said Charles Getty, director of information security at York-based Business Information Group. "But it's not unusual for small- and medium-sized businesses to balk at doing that. They often don't seriously consider it until they get hit."

Besides doing a cost-benefit analysis, there are other considerations, he added. "In general, companies can use 'cluster technology' [a set of connected computers that effectively work as a single system] as a kind of 'fail-safe system,' so if one goes down, others will take over the load," Getty noted. "But the challenge there is that if one gets compromised, say by ransomware, the threat can quickly spread. One solution to that is to have a separate, offline backup too, but that can take time."

The best approach, he said, is to "assess your risks — from cyber threats to natural disasters — and consider the impact on your business operations. Then consider the possible solutions and how they fit with your budget."


Keath

One of the quandries facing businesses is the dichotomy between security and productivty, pointed out Brandon S. Keath, cybersecurity practice lead at Mechanicsburg-based Appalachia Technologies LLC.

"Technology can be considered as a door that helps companies get their goods and services to market easier and faster," said Keath, who also runs PAHackers, an "ethical hackers" organization. "Security is the lock that guards things. But when you put a lock on a door, it's tougher to get through it to make your delivery."

Once a business comes to terms with that, Keath said it should "invest in redundancies and periodically test" the systems. But many companies don't have a backup plan, or its limited, or they've never tested it, he added.

He also noted that high turnover among technology professionals compounds the problem.

"Something happens and no one knows exactly how the system works, because the person who designed it is no longer there," Keath said. "This happens in small companies and multibillion-dollar ones. Businesses need to properly document any changes or additions to the IT system." ■

The best defense

A hardware or software vulnerability in a computer system is, in reality, a mistake made by its designer, according to Ronald C. Jones, a cyber security instructor at Harrisburg University.

"Each company that designs computer system has a cost-tradeoff point where more vulnerability testing decreases the profitability of the computer system," he noted, highlighting some best practices that can help to reduce the number of mistakes in a system.

"Use software fuzzing," he suggested, referring to running a program with a wide variety of "junk" input that can highlight abnormal or other unexpected results.

Another is to utilize "common criteria," which refers to products that can be evaluated by competent and independent licensed laboratories that can determine particular security properties.

As an additional precaution, added Jones, companies may consider "third-party review by someone who was not involved in designing the computer system."

In Target's case, the cash registers "suffered from a systems design flaw, a monolithic design which created a single point of failure," he said. "Target was not clear but inferred it was some type of computer system design. It is cheap to build and operate a monolithic system, that is, until it fails. The best-practice approach is to have redundant systems and have half of the company operated on one side. Another approach would be to operate on one system on even number months and the other on odd number months."

There can be a big tradeoff between productivity and vulnerability when it comes to designing computer systems, according to Andrew Hacker, Harrisburg University's cyber security expert in residence, and CEO-founder of Thought, a blockchain technology company. "New and improved technology can bring significant productivity enhancements, but it can also bring cyber security and other risks."

The problems are not limited to Target or other retail chains, he added. Hacker pointed to mobile phones as an example, noting that "cybersecurity was not considered a problem when they were introduced." But now, with smartphones holding banking and other sensitive information, "more threats have emerged."

His suggestion: "Bring in internal or external cybersecurity partners as early as possible."

Hacker, who previously worked as the deputy to the state of Pennsylvania's chief information security officer, said technology security personnel "were at the table early on as each department rolled out new projects. It may cost a bit more, but this approach provides more security."

To minimize the chances of a systemwide failure, Hacker said, companies should consider installing redundant and hardened, or secure, systems.

"You do have to consider the cost, but also consider the cost of downtime," he noted. "Also, when your systems interact with an outside provider, take the time to test their compatibility. In the beginning, most systems were closed, but now it's common for external vendors to be hooked into a company's system, so there's a greater need to review the systems, maintain their continuity and consider backup plans."