MEET THE PANELISTS

DEVI MOMOT

CISSP®, GSLC®, GISP®
CEO
Twinstate Technologies

Devi Momot is the CEO of Twinstate Technologies. An award-winning certified Women-Owned Business Enterprise on the federal level and in New York, Vermont and New Hampshire, Twinstate Technologies is recognized for its 50-year legacy of innovation, entrepreneurship and exceptional customer experiences. Devi is a Certified Information Systems Security Professional (CISSP®) by (ISC)2, the International Information System Security Certification Consortium Inc. Certifications by (ISC)2 are internationally revered. She has core cybersecurity leadership certifications from the SANS (SysAdmin, Audit, Networking and Security) Institute, including the GIAC Security Leadership Certification (GSLC®) and the GIAC Information Security Professional (GISP®). She serves on advisory councils for global tech titans including Sophos and is a present and past member of a number of boards of directors.

TWINSTATE TECHNOLOGIES®

JAMES POMPILIO

Vice President of Security & Infrastructure
Garnet River

Jim has more than 25 years of experience in the technology arena, focusing on IT strategy, security, operations and the complex needs of regulated entities. Jim has practical experience in information and physical security systems management, business development, application and product development, project management, sales and marketing. His strong business acumen, functional knowledge and ability to acquire and administer resources instills trust and accomplishes an organization's mission. Jim works closely with senior executives of Garnet River's clients to help design, build and support increasingly complex infrastructure, products and services. He has experience consulting, designing, developing, delivering and managing offerings for Fortune 500 and Global 500 companies as well as the Department of Defense, federal and state government entities. Jim is also president of InfraGard Albany, which is a partnership between the FBI and the private sector that helps protect the physical and cyber infrastructure of the United States.

Garnet River
A Full-Service IT Company

TABLE of EXPERTS

DATA THEFT

The *Albany Business Review* hosted four experts to discuss data theft. The discussion was moderated by Sierra Kehn of the *Albany Business Review*.

What exactly is data theft?

James Pompilio: Data theft is the deliberate or intentional act of physically or digitally stealing information.

What are some of the most common modes of data theft?

Craig Skevington: There are three different ways or intents. One is to basically steal your resources, where you have computers that are sending out emails and spamming. A second way is to actually steal the data, so they're getting Social Security numbers, birth dates, and other personal information. The third, which we see most often, is coming in and corrupting your data to force you to pay them in order to get your data back.

Adrienne Terpak: We see businesses experiencing a fair amount of fraudulent activity with business email compromise or, as it's also known, CEO fraud. Typically, fraudsters will monitor the corporate email environment in the background for a period of time, learning how employees communicate with each other. The use of social engineering allows the fraudster to deceive individuals into sharing confidential information or simply executing an urgent wire that they believe was requested by an executive of the company. A cybercriminal may send a phishing email including a link that compromises not only the recipient's computer, but can spread to others on the network. We also see incidents where a fraudster poses as an existing supplier and establishes a good working relationship with someone at the company. After gaining the employee's trust, the criminal may provide new banking instructions to divert payments or provide fake invoices to redirect them.

Why is it important to have a planned response to a data breach?

Devi Momot: It's important to have a plan because there are two outcomes that can happen: a good one and a bad one. If you don't handle them in a proper method, you can actually harm your case if it's truly a case. If you do missteps, you can increase the damage to the organization over what it could be, or you could decrease your chance of prosecution, should there be an opportunity to put some bad actor away.

Too often we see that people are quick to make a decision on something in regards to a response. They're not necessarily qualified to make the decision and they've ruined the opportunity to either save their organization a lot of money, time and embarrassment, or put the bad actor in jail or at least get them labeled with the appropriate misdemeanor or felony so that their background check doesn't come out clean.

Pompilio: It's going to be very stressful once it occurs, and you're going to need some sort of guidance to walk you through the process. It's just a plan, and things are going to be completely different when the incident occurs. Having a plan is something to follow and keep you somewhat calm during a very stressful situation.

Skevington: I would just add that you need a plan. It's not if it's going to happen. There is no way to prevent a data breach from happening and it's getting more and more common every day. It's going to happen, and when you have your business shut down and you don't know what to do, that's a problem.

How likely is it that an organization will experience data theft?

Pompilio: Given an appropriate amount of time, it's 100%. It's going to happen. I would venture to guess that anybody that has a business today has been breached. It's just, to what level? Everybody has sales people that have probably left with sales lists. You need to understand what your assets are and what the risk is to those various types of things once they are stolen. Some of them have a higher cost or a greater impact than others.

What should companies do if they detect a security breach and how can they recover from a data compromise and/or loss?

Terpak: A recent Treasury Perspectives study spon-

Craig Skevington, left, James Pompilio, Adrienne Terpak and Devi Momot.

DONNA ABBOTT-VLAHOS

sored by TD Bank revealed that, although commercial clients are aware of cyberthreats and are very concerned about the potential impact of a security breach (74% of corporates see it as a priority v. 92% of bank respondents), they're not fully versed about the various ways they can prevent them from occurring. The key is to avoid being in reactive mode all the time. TD takes a proactive approach with our clients to understand their environment and operations, and learn what security policies they may already have in place. Then we informally consult with them to create a risk culture – addressing the human layer of security – to implement.

If a breach does happen, it's very important to alert whoever internally is part of the security team. You should alert the CIO or CISO, if there is one, and the authorities, if it makes sense. In addition, the FBI has valuable resources including the Internet Crime Complaint Center (IC3) to track these events. Although they may not be able to investigate or solve a particular case, they're analyzing and tracking criminal activity data that could help your company or someone else in the future. Of course, notify your bank immediately if your accounts have been compromised. We can lock down your accounts, work with you to change account numbers and make sure the appropriate products and services are in place to help thwart fraud or theft.

After the immediate threat has been managed, it's time to regroup and look at policies and training. It is critical to create a culture around security so that everyone incorporates it in their daily lives.

What are the greatest security risks that a business faces?

Skevington: Employees. Forty-eight percent of breaches are caused by employees. Most of them aren't intentional. Employees are not educated to know what to look out for and the phishing scams are getting much more sophisticated. Hackers are even using local banks and sending out phishing emails under their monikers. Employees need to be trained on passwords. Dropbox was supposedly breached a few years back and they found out it wasn't Dropbox. It was other less secure sites that were breached. Hackers know that most people use the same password for all of their accounts, so they go into less secure accounts, get the passwords and then attack the more secure accounts that contain more valuable information. People are the issue.

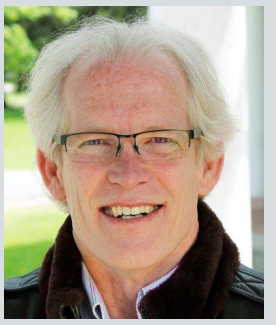
Momot: There are some applications coming out that are really helpful. The less we can present to our employees that's bad, the less chance we have of them acting on it. The likelihood of them acting on something that's bad, even after we train them to remarkable degrees, is almost 100 percent. A Verizon report showed that one in 24 will click on a phishing email. If you send out 24 emails in an organization, the likelihood is that you'll get at least one click. We have never, in all the training that we've done, gotten to zero percent. The less you can present to the employees, the better. And know that IT has access to everything. They've got the administrative credentials and they have access to everything.

Pompilio: Everybody's always worried about the people on the outside. You do have to look at the people you let through your doors every day. There are people that will make mistakes or click on something by accident, which can certainly lead to something. But there is also the potential for a malicious actor or somebody who was going to leave or a disgruntled employee or an intellectual property thief. We had a local GE Power employee in the news recently for allegedly stealing trade secrets. It happens. It takes constant monitoring. There are a number of tools to mitigate loss; policy, procedure and technology. But you really need to understand what your assets and your risks are, and then prioritize them and work on protecting them from your greatest risk down to your least.

How can security keep pace with increasingly sophisticated and creative attacks?

Momot: Teamwork. That's the biggest thing. It requires the banks, the competitors, all of us at this table, to band together. Not every manufacturer in security is of high integrity. Some of them have alternative motives, but we do band together in this space

MEET THE PANELISTS



CRAIG SKEVINGTON

Founder, CEO & President STEADfast IT

Dr. Craig Skevington, a serial entrepreneur, has created multiple high growth companies across different industries: manufacturing, health care and information technology. His first company, FACT, was the 236th fastest-growing company in 1994 and ultimately became a publicly traded company. His second company, Flow Management Technologies, was the 79th fastest growing company in 2002 and currently serves over 1,100 physicians. Borrowing from workflow concepts learned from other industries, his current company, STEADfast IT, is growing rapidly as it evolves from a local market to a national footprint. The business model is built on a proprietary ticketing process which enables STEADfast to provide industry-leading response times and a new standard for IT service delivery. Last year, Craig won the Center for Economic Growth's Jeffrey A. Lawrence Lifetime Achievement Award. Beyond his startups, Craig enjoys challenges such as scaling Mount Kilimanjaro, completing an Ironman triathlon and flying seaplanes.

STEADfast IT

ADRIENNE TERPAK, CTP

VP, CSB Segment Manager Treasury Management Services, TD Bank

Adrienne started her career as a corporate treasury practitioner and held senior management positions at Prudential Financial and Sharp Electronics Corp., with responsibility for treasury operations, accounts payable and accounts receivable. She has worked at TD Bank for 5+ years and currently manages the corporate and specialty banking segment for treasury management services, directing the growth strategy for large corporates, corporate real estate, asset-based lending and dealer commercial services. Adrienne has presented at industry events including the NACHA Payments Conference, CFO Treasury Management Summit and the New York Cash Exchange on topics such as corporate payment strategy, payment fraud and cybersecurity, SWIFT, and treasury management system integration. She holds an MBA in finance from Seton Hall University and a B.S. in Spanish/business administration with honors from Pennsylvania State University. Adrienne is also a Rotarian and steering committee member for the Women of Commercial Banking and Treasury Management.

TD Bank

America's Most Convenient Bank®

Adrienne Terpak, left, James Pompilio, moderator Sierra Kehn, Devi Momot and Craig Skevington.

DONNA ABBOTT-VLAHOS

very much and are hand-in-glove with the IT people of the organizations that we serve, as well as the executives. My hope is that by reading this article, the executive levels start to get more involved because that has been a missing link. They really need to know what the environment is so that they're part of the mix, part of the team.

What is the bank's approach to helping clients tackle cyberthreats, and how has that approach evolved with the ever-changing environment?

Terpak: In addition to fraud prevention services, such as check and ACH positive pay, and multi-factor authentication, financial institutions can provide guidance and tools to educate and support our clients' cybersecurity programs.

TD Bank's approach includes in-depth conversations with our clients about their operations and technology, providing web-based links to fraud prevention resources, hosting topical webinars, sharing industry and peer surveys, and conducting informal consulting engagements, all at no cost. We also recommend best practices such as daily review and reconciliation of bank accounts, segregation of duties and security training for all employees, to name a few.

These practices are especially critical for companies to employ as part of their M&A activities. For instance, the acquirer should address the consolidation of accounting systems, or multiple versions of it, as well as ancillary systems for treasury management and accounts payable. It is also important to promptly review the acquired company's operational procedures and security policies, bring them into the fold, and investigate whether there are any pre-acquisition breach events that need to be addressed.

What are the top three challenges that companies face when trying to secure their data?

Pompilio: No. 1: They lack security leadership at the top so that they can be proactive and mitigate their losses. That's a difficult thing for some organizations. They don't have anybody to do it or they just name somebody because they happen to be the technical guy.

No 2: Is they don't fully understand what assets they have that could be stolen. It's important to understand that these could be in digital or physical form. Somebody could walk out the door with intellectual property in the form of physical plans, just as easily as they could email them. Understanding what they have, what their business partners have, and what they store out in the cloud is important.

Lastly, they lack formalized policies and procedures and, just as important, the enforcement of them both.

What immediate actions should companies take to protect themselves?

Skevington: Companies really have to begin training immediately. Certainly, an assessment of their technology including firewalls and all internet connection points would need to go along with it. The Iranian nuclear program was hacked into a number of years ago and that facility wasn't even connected to the internet. They had no connections to the outside world, but the hackers, allegedly the U.S. and Israel, knew that people were the weakest link. And so they used thumb drives because they knew that people were going to be curious enough to plug them in. They did. And the hackers went after the suppliers who were less secure than the nuclear facility, and they got in there. When they ordered a new hard drive, it was delivered with the virus already on it and they didn't know it. It did a tremendous amount of damage.

It's going to happen. You can't protect yourself but you need to do the training and make sure your employees reduce that risk as much as possible.

Can a small business afford to implement these security measures?

Momot: Years ago, not so much. Today, absolutely. The capability of managed security services providers in the space and the organizational structure allows the sharing of very specifically trained and resourced teams of security professionals. The important thing to remember is that anybody that has administrative domain admin rights has the keys to your castle. Make sure you're doing background checks. One very well known breach is Home Depot. Their IT guy had a felony. Anybody that's got access to keys to the castle ought to have a background check, whether they're on your staff or the vendor's team.

Pompilio: You need informed security leadership. Not everybody is security-aware in an organization, and they will never be 100 percent aware. Some people get it. Some people don't. You need the right people at the table, and there are security staffing resources available to organizations that can help them. If they don't feel they need to bring in somebody full time, they can rely on resources on a fractional basis – part time for their needs.

Start at the top because it would be like trying to institute a four-day workweek on your own. It is never going to happen unless you talk to executive management. You need their buy-in. You need their commitment. Otherwise you're spinning your wheels.

What are some of the best things consumers can do to protect themselves?

Skevington: Consumers need to become a little more knowledgeable of what they're up against so they can spot these things as they come in. Another is to change your passwords. They've done studies with large groups of consumers and found that something like 35% of people were using the same password across multiple sites. It was 1-2-3-4-5. A lot of sites are getting better at forcing you to establish a safer password, but even there, a lot of people use one password across all their accounts. And every account has a different level of security. It's getting to be a routine practice of hackers to go after the sites that are less secure and then use that information in the ones that have the security. Passwords are a big thing. Make them all different. Every 90 days, change the password.

Don't keep all your data online. Get it off your laptop. If you're not going to be using it, put it out on a disk somewhere and store it. The more information you have that's readily available to people, the more at risk you are.

Momot: Be paranoid. Help your seniors and your less able friends and neighbors. We had a really awesome friend, 90-year-old vet, and through email he got scammed out of over $100,000. It wasn't until his daughter walked into a bank – they probably breached some confidence rule or something – and said, "Do you realize a lot of money's leaving your father's account?" You hear these stories and it really makes me angry that the creeps and cheats and thieves out there take advantage of the ones that are the most loving and caring and trusting in our community. If you have the capacity to learn, learn. Use multifactor authentication and then help those in your community that just don't have that capability.

What does the bank find most challenging about helping clients create and maintain an effective cybersecurity regimen?

Terpak: Clients need to feel that they can take ownership of their own cybersecurity. Day-in and day-out, they are exposed to communications and exchanges that could provide an opportunity for a breach, even at a later point in time. The challenge is increasing awareness of how and to see that they need to really focus on each step of the operations and what extent they might be vulnerable; to make sure they're following the prescribed security policies; and to perform regular reviews to ensure that their finances and information are thoroughly safeguarded.

Something else to consider: access to bank applications and accounts should be closely managed and audited. Employees that need it should be granted access with the appropriate entitlements, and for those who need display only, access should be limited to that. Companies must always monitor and adjust employee access as necessary.

In addition, banks can send customer alerts when transactions are made on their account or install an electronic (soft) token whereby the security is embedded in the system – anything to make it easier for the client to manage. Personal "challenge questions" for authentication are another layer of security.

Momot: It's the idea of multifactor authentication. For example, if it's a physical entrance into a facility, it's having two different methods to verify that

that's who's supposed to be able to come in and that's who we expect is going to be coming into that physical property. Digitally as well, LinkedIn, Facebook, all these applications now have multifactor authentication.

"Positive pay" is another multifactor authentication. We paid a bill to a company based in Newmarket, Ontario. Next thing we know, we're getting a call from Chase Bank in California from an agent who said, "Hey, this just doesn't seem to add up." Normally, they'd never make that call, but that check was $350,000 which started out as $850, and written in Ontario. The check got physically stolen somehow and was deposited into a trust account, which I guess would be a little bit more difficult to get money from. We instituted positive pay after that point, which is a point of multifactor authentication: You write the check, it goes through the process and then the bank contacts the issuer of the check to verify that it's authentic.

Terpak: I would add that it's well worth the nominal cost to activate positive pay, for checks and ACH, versus suffering a loss and trying to recoup those funds after the fact. Banks will do everything possible to recover funds but it may not always be successful, despite our best efforts. That's why it's critical to heed the advice of your banks and technology providers to avert a compromising situation, breach or theft.

Can you talk about 'hard token' and 'soft token,' and how they play into this conversation?

Pompilio: In relation to system access control, there are three common factors used for authentication: something you know, password; something you have, hard or soft token; and something you are, biometric method. Multifactor authentication uses any two or more factors. An example would be once you enter a password on your computer to access a system, you are then prompted for a "one-time code" displayed on the "token" to complete your access. A card or key fob is an example of a "hard-token," but apps exist for smartphones that are considered "soft-tokens." The idea is that since the "one-time code" is delivered via a token "out-of-band," that is not on the computer you entered your password on, you are safer if your computer is ever compromised. It is a relatively easy security measure to implement. Your banks, social media and many other online services offer multifactor authentication.

What we're talking about is added steps, more procedures, educating yourself and being aware of these types of things. What typically happens is, because it is an extra step, people take the easy route. It's why they have one password for everything. Remember, everything's always fine right up until it isn't. You need to plan. You need to do these things to keep the bad things from happening because your business may not survive, or your life savings may not be there when you go looking for it. These are important things that people can do. They're relatively simple, but they do take a change of culture, attitude and personal responsibility. It's not somebody else's responsibility. It's your own.

How can creating a culture of cybersecurity be a competitive advantage for a company?

Momot: They stay in business, more likely. That's a big competitive advantage. I think, too, from a third-party perspective, if you've got a good security culture, talk about it. Talk about what you've done to protect the assets. Let's say I'm a third party and I work with TD Bank or either of the other companies represented here today. They're going to be more likely to do business with me if I'm a good steward of our connectivity and our security and our privacy within our firms.

Pompilio: Mitigate your risks so you become a better organization, one that makes you more attractive to customers and business partners. People do not want to conduct business where they don't feel safe. It is important to know that outside of the U.S., there are countries where hacking and data theft is their business. There are certain countries that are better at hacking certain types of systems, and certain criminal organizations and nation states that are looking for intellectual property just to capitalize on it, copy it and replicate it for their own benefit. They don't need a "research and development" division, all they need is a hacking team to go steal somebody else's idea. When we think of business, we think of business as a legitimate activity. It's important to understand that there is an illicit underground economy where this is occurring. Our job is to protect ourselves from it.

Skevington: It gets back to what we did with the Iranian nuclear program. We didn't go after them. We went after their suppliers and the suppliers of the suppliers and it was very effective that way. It's a whole chain. You can't just protect yourself. You have to look at everything that you're bringing in, and think, how well protected is that data?

Terpak: If you can demonstrate that you have a robust discipline around evaluating your strategic partners, especially for the bank, it's really important. For instance, there is a lot of opportunity to partner with fintechs. If a financial institution can't build a capability in-house, for example, they collaborate with other companies to offer resources that our corporate clients might not have access to. We make sure that the solutions we deliver to our clients have undergone the most vigorous evaluation possible. Demonstrating that discipline builds a competitive advantage and trust with our clients – that we understand the process and what we're bringing to the table has been fully vetted.

What would you like readers to take away from this conversation?

Skevington: Everything we've been talking about is really just the tip of the iceberg in terms of what's going to be happening in the future. Everybody's after financial information and money has been a big driver in all of this. But take, for example, Iran's nuclear program. We didn't go in to corrupt data. We went in to take control of actual equipment. We took the centrifuges and spun them up until the motors burned out. That was a whole new step, a whole new evolution of hacking.

One hacker proved that he could go in and take control of a Jeep's brakes and transmission and essentially control a car that's driving down the highway remotely. He demonstrated his findings to Jeep to show that they had vulnerabilities. If he wasn't that honest, that could've been a real problem.

Look at the next step. We've got all these programs like 23 and Me and the genetic tests. All that information is going into a database that's being shared with pharmaceutical companies and law enforcement. It's one thing to lose your Social Security. It's another thing to lose your genetic code.

Terpak: It's encouraging that we're collaborating with clients and technology partners, and having more of these conversations on a regular basis. Awareness must be built internally as well as externally, and it really behooves us to bolster the human layer of security and frequently share whatever information we can. Cybersecurity will continue to be a growing concern because fraudsters are always exploring new ways to infiltrate systems. If businesses and banks tackle the issue collectively, it makes combating cybercrime easier and more effective.

"It's not if it's going to happen. There is no way to prevent a data breach from happening and it's getting more and more common every day. It's going to happen, and when you have your business shut down and you don't know what to do, that's a problem."

CRAIG SKEVINGTON, Founder, CEO and President of STEADfast IT.

TRANSCRIPT LIGHTLY EDITED FOR SPACE AND CLARITY.

Thank you to our participants

Garnet River
A Full-Service IT Company

STEADfast IT

TD Bank
America's Most Convenient Bank®

TWINSTATE TECHNOLOGIES®