TABLE *of* EXPERTS

CYBERSECURITY THREATS

WHAT TO LOOK FOR, HOW TO PREPARE

ISTOCK

MODERATOR

Ryan Weber

PRESIDENT
KC Tech Council

Ryan currently serves as President of KC Tech Council. Additionally, Ryan serves on the board of the Technology Councils of North America (TECNA), and is a member of the executive mentorship program for the College of Business at Kansas State University. Ryan further demonstrates the value he places on staying involved in the community by supporting several other organizations in the region and is a 2015 graduate of the Centurions leadership program.

PANELISTS

Jake Gibson

CHIEF SECURITY OFFICER & CHIEF COMPLIANCE OFFICER
Lightedge Communications

Lightedge Communications, Chief Security Officer & Chief Compliance Officer

With more than 20 years in the information technology field, Jake brings a proven record of leadership excellence and extensive experience in process improvement to LightEdge. Jake has served in IT leadership positions across several industries including; healthcare, insurance, pharmaceutical, and food.

Throughout his career, Jake has been involved with aligning security and compliance initiatives with business objectives. With his cross-industry background, Jake focuses on developing, implementing, and supporting LightEdge's strategic security and compliance vision.

Michael Hannan

MANAGER – TECHNOLOGY RISK SERVICE PRACTICE
CBIZ

Michael is a Manger in the Business and Technology Risk Service Practice in Kansas City. Since joining CBIZ in 2008 Michael has led a number of IT risk assessments, general computer control reviews, Sarbanes-Oxley Section 404 projects and third party internal control attestations. He has a Bachelor of Science in Business Administration/Accounting, concentration in Information Systems from the University of Kansas. Michael has affiliations with Certified Information Systems Auditors, Institute of Internal Auditors and the Information Systems Audit and Control Association.

Zach Hargett

SOLUTION DEVELOPMENT ARCHITECT
ISG Technology

Zach brings ISG Technology more than 11 years' experience in designing, implementing and supporting highly available network systems and solutions that include diverse network technologies and capabilities. Primarily focused on storage, compute and virtualization, Zach works with large Enterprise network architectures, designs and systems. Success stories include relieving bottlenecks or contention in existing environments and building innovative systems that far surpass previous hardware. He holds a B.S. in Information Technology from DeVry University and is located in Overland Park, KS where he resides with his trusty pal Moose, his chocolate Labrador.

Tedrick Housh

PARTNER
Lathrop & Gage

As chair of the Data Privacy and Security practice group at Lathrop & Gage, Tedrick Housh practices at the forefront of rapidly developing legal issues relating to the digital economy. He is a leader of the firm's work on data privacy, data security, risk assessment, prevention and data breach issues and assists clients with the technological, logistical and legal issues arising from the loss or disposal of personally identifiable information and personal health information. He holds a Certified Information Privacy Professional / United States (CIPP/US) designation from the International Association of Privacy Professionals. He has maintained an extensive employment litigation practice, and serves as a firm leader in that area.

ADVERTISING SUPPLEMENT TO THE KANSAS CITY BUSINESS JOURNAL

CYBERSECURITY THREATS

Cyber threats against American businesses are increasing in frequency, scale, sophistication and severity. Cybercrime has jumped 38 percent, with global costs to businesses projected to exceed $2 trillion by 2019.

Businesses' best defenses, however, often are decidedly low tech. Employee awareness and training plus board-level engagement are among the most effective ways to mitigate your company's risks.

Area cybersecurity experts shared these and many other insights during a recent discussion hosted by the Kansas City Business Journal. *Ryan Weber, president of the KC Tech Council, moderated the discussion designed to help Kansas City businesses—from small to large—prepare for breaches and contain the damage they cause.*

Ryan Weber of KC Tech Council: **What steps should board members and upper management be taking to lower their risk of cybersecurity threats?**

Michael Hannan of CBIZ: First, they need to be aware of cybersecurity. Every cybersecurity presentation these days starts with Target. As most people know, Target suffered a massive data breach in 2013 that affected about 70 million customers. Several lawsuits were filed, including one in which plaintiffs claimed the company's board failed to take sufficient steps to protect the company from cyber breaches.

This summer, a Minnesota court dismissed the lawsuit against Target's board, ruling that Target's shareholders and management took the necessary precautions. They had policies and procedures in place related to cybersecurity. They did proper vendor management. They were doing social engineering testing. They had cyber liability insurance.

But it shows that C-level management and the boards of companies need to be cognizant of cybersecurity to protect themselves as well as the company itself. By taking these steps, the hope is that repercussions are limited when breaches occur.

Weber: **You mentioned cyber liability insurance. How much of the damage is covered if cyber breaches occur? What should companies know about these types of insurance policies?**

Hannan: Like any insurance policy, cyber liability insurance obviously doesn't cover everything, and there are loopholes in policies that allow companies to not be protected. So insurance is good for companies to have, but they should not rely on that solely. The controls, policies and procedures, and testing should be the focus for companies. The insurance is just part of the incident response plan. It's just your safety net to mitigate your company's exposure when breaches occur.

Weber: **Tedrick, tell us about the legal side of cybersecurity and best practices for companies to protect themselves.**

Tedrick Housh of Lathrop & Gage: Target is a good example of the types of liabilities and suits you will face in the aftermath of a breach. There were shareholder derivative suits that were brought against the board of directors. There were class action suits brought by those consumers who claimed they had been harmed, and then there were suits by the banks or the issuing credit card companies who wanted to recoup the money they had to pay to all those consumers.

With the shareholder derivative suit, best practices can help protect you—regular board meetings where this is a topic, committing resources to cyber protection, showing that you were not asleep at the wheel or had your head in the sand.

What's interesting to me from a legal perspective is that class actions from consumers are growing. In the past, the courts had generally said that if you just have a fear that your identity might be stolen because it's out there, you don't really have injury for purposes of bringing a suit. Target and some other court cases are now putting some cracks in that wall to say that spending personal time worrying about your information being stolen or suffering some expense from finding out whether your information has been compromised can constitute injury. So that means class action suits of consumers can generate a lot of attorney fees even though there may be very little amount of actual damage.

That's why insurance ties into this. Cyber liability insurance is one of the fastest growth areas in the insurance industry. The underwriting of it or the setting of rates and what the policies actually say are still very much in flux.

As a law firm, we work with our clients to look at the policies before they purchase them—not just price but what clients get for their dollars. Do you have first-party coverage for the things that happened to you or third-party coverage for the things that happened to others for which you might be responsible? All of those issues get rolled in together. Terms and how items are defined are very important. If there's something you want, you want to make sure you state it specifically so you don't end up with problems later.

Weber: **So language is very important. What are some other things companies could do to prepare?**

Zach Hargett of ISG Technology: It's not just about protecting the perimeter anymore. It's more than throwing up a firewall or a certain piece of technology on the outside. The ways of conducting business have changed. You think about Gen Mobile and how people are always on the go and always connected. That just gives attackers more opportunities.

There are vulnerabilities everywhere, when data is at rest or in movement or being accessed through an application. Encryption is big. Protecting data is probably one of the bigger concerns we help companies address. It's no longer a

ADVERTISING SUPPLEMENT TO THE KANSAS CITY BUSINESS JOURNAL

CYBERSECURITY THREATS

matter of "if" a cyber breach happens. It is a matter of "when."

Weber: Companies are looking to groups to provide audits and assessments of some of their cybersecurity needs. How often should that be conducted?

Hargett: A couple of times a year is a pretty good practice. Or if you go through some sort of infrastructure change, whether that's internal or external, you want to make sure that your ducks are in line after that change takes place. Having somebody outside of the implementation team come in and conduct that audit is a good means of checks and balances.

Weber: What are other ways companies can protect themselves?

Jake Gibson of LightEdge Solutions: The biggest area for me is employee training and awareness. A lot of the breaches come from the weakest links. Many employees aren't aware of the risks of their actions. They see an advertisement in an email, and it's just habit to click on that and follow that link through. Identifying those suspicious ones is important, which means really educating our employee base.

Another important component is having a good risk assessment methodology. I think a lot of companies try to protect everything. You're never going to win protecting everything. But by identifying what your risks are and what your biggest gaps are, you can prioritize your method or your list of attack methods to mitigate those.

Weber: What do you see as the next wave of cybersecurity tools?

Gibson: Tools are coming at us left and right. There're always new advances, new company startups. Even the big companies are coming out with new products all the time. I think if we chase those, we're going to lose. We really need to have more of an encompassing security practice around it. We need to leverage those tools to fill those gaps that we identified through our risk methodology.

A lot of our companies don't have the in-house technical expertise to handle this, so we're partnering with IBM. They offer virtual security operation center services. We're leveraging them to actually pull and analyze these log files regularly. We're analyzing these threats in the industry and comparing them with what they're seeing on their own network. It helps you identify some of those weaknesses as well.

Weber: CIOs and CTOs are being sold new tools every day that are supposed to solve all their problems. What should decision makers look at before pulling the trigger on those tools?

Hannan: The social aspect is your biggest weakness right now. You can have all of the technical defenses but all it takes is one person to click on something to compromise your system. So training to that aspect or testing to that aspect which includes social engineering testing are important.

Then the other big aspect is just the internet of things. We're seeing it across all industries. In manufacturing, for example, they have control systems throughout their entire plants. Every single one of them is networked, either hardwired or wirelessly, and those are all access points.

Healthcare is another example. Every single device in each healthcare facility is networked. It makes providing healthcare easier, but the devices are all access points. When we come in and ask them where their access points are, they say here's our IP listing. That's it.

That's not it. You have to do device inventories and information inventories. What information do you have on site? Where is it? Does each employee have some? Is it contained in certain folders? Identifying where you have that information and securing it is important.

A lot of companies only think of customer or client information. That's what they're locking down. But they also have personal information about their x number of employees. That kind of breach hurts your reputation just as much as if you had a customer breach.

Weber: What are some of those best practices that companies should be implementing now and then when something happens?

Hannan: It comes down to people, because people are the ones who typically make the errors. For example, one company has created a social engineering solution to counter the risk of people clicking on malware links inside of emails. They made it so that employees can't open links within emails. Instead, they have to copy and paste the URL into the browser. It takes longer but it creates another moment in which you might stop someone from inadvertently doing something harmful.

With respect to technology, if you're on the board of directors of a Fortune 500 company, you don't know any of this technical stuff. The issue is, have you reasonably looked for resources to determine whether you mapped your data correctly and whether you have the appropriate technology answers for the type of risk and priorities you've identified.

Weber: I actually don't ever think about board directors being liable for some of this. But certainly they have that fiduciary responsibility. I bet many don't know that.

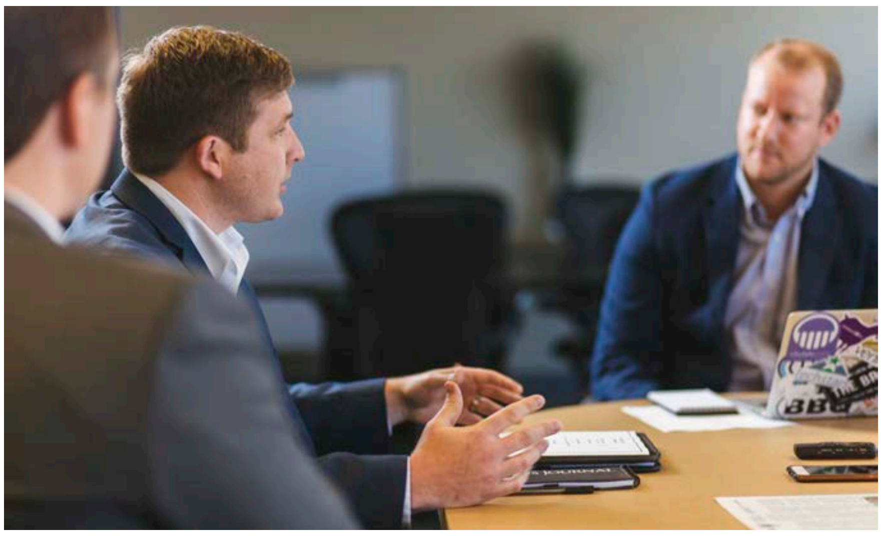
Gibson: A lot of them don't. I frequently present at the New York Stock Exchange Governance Services programs on both coasts. Board directors always want to know the risk associated with being a board member.

When you think about it from a board perspective, you're at a higher governance level. Your solution typically is to take action against the C-suite and to get rid of your chief technology officer or CEO. But that isn't the end of the line when you have an issue that has affected the stock market

CONTINUED ON PAGE 4B

ADVERTISING SUPPLEMENT TO THE KANSAS CITY BUSINESS JOURNAL

CYBERSECURITY THREATS



ANDREW GRUMKE

CONTINUED FROM PAGE 3B

price of your company.

Weber: How important is it that is that key top people are engaged in this conversation? Your C-level people are often the targets of this, right?

Hargett: Right. That's sometimes a struggle, too, because the board and the C-level employees often want to be pulled back a little bit from that. It seems like the only time they're being brought in is after the fact. That's unfortunate because they are the ones who are responsible when an action is not being taken that should've been taken. It's a struggle. We interact a lot with the hands-on folks, the directors, managers, administrators and engineers. But we're always making sure to bring in the CIOs and the CFOs and the CTOs. We offer presentations to the C-suites.

Weber: How granular do the reports to the CEO or the board need to be? Is the presentation to the executive officers more detailed than your presentation to board of directors or is it the same?

Hannan: Right now, we're telling companies that it should be the same. We do National Institute of Technology and Standards cybersecurity assessments. Those speak very heavily to the board of director interaction and the reporting they get. That part of our testing is on a quarterly basis.

On a monthly basis, however, you should try to present as much of the granular information as possible—here's what's going on and here are the changes we're putting out. Be as detailed as you can get with them and bring them up to speed on what the environment is.

Weber: So the CEO should be regularly receiving a dashboard kind of a report from the chief of information or security officer. What does that report usually contain?

Gibson: A lot of times, they are incident reports, the number of incidents and types of incidents that you've had, any new risks that have been identified, and any remediation actions that have been implemented. There's a lot that goes into those reports, and often, you get a lot of blank stares. But it does bring the attention level up in the room. They start to become more cognizant of the security landscape.

Hargett: I think that you still have to cater a little bit to your audience. You have to know their background. If you've got a CIO that is very technically sound, you should be aware of that and use that to your advantage. But if your CEO has that deer-in-the-headlights look, you have to learn how to talk to them and make sure the point is getting across.

Weber: Can you share some real life examples of cybersecurity threats you've dealt with?

Hannan: Ones we're seeing right now and most of the ones that get perpetrated are related to simple email phishing. Several companies, for example, have had hackers asking employees for W-2s at the end of the year in fraudulent emails.

Wire transfer and ACH fraud are also common. I get a call once a week from a client about fraudulent ACH requests. Hackers know when the CEO is out of town. The email signature looks exactly the same as the one used by management. They know the way he composes emails. It's like they've been watching their emails.

The CEO of one of our clients was out of town. He is normally the wire transfer requestor. It's not abnormal that an email comes from him. The language looked perfectly correct and said, "Can you wire $100,000 by the end of the day? I approve it, but I'll be out of touch the rest of the day on vacation."

It made it through. They called the bank only after the CEO happened to check in later that afternoon to see how things were going. They said: "We got the wire from you. It's taking a little of time. But we'll get it through." And he told them he never sent the wire request. It made it through their multistep system. It took him calling in and checking and then calling the bank to see if they could stop it, which they did. But we've had other clients who have fallen for it.

Weber: How did they know that they're out of town?

Hannan: That's a good question. With the type of information they have, you have to think that they are already in the system and watching their emails. They know too much.

Hargett: We hear a lot about ransomware.

Weber: What is ransomware?

Hargett: That is when a set of data has been basically encrypted, and it's made unavailable to the company. A set of data being locked out can make an entire system unavailable. I think ransomware instances are only going to continue to increase. It's a matter of risk and cost and how that relates to reward. As long as the risk and cost are lower than the reward, you're going to continue to see this type of activity because it's super easy to pick off the low hanging businesses, and they'll compromise on a price.

Weber: Is there any guarantee that a company gets that data when they pay that ransom?

Hargett: Absolutely not. We've heard about that in the news where folks will fork over x amount of money thinking this problem will just go away only to either be hit again later or not get the key to unlock their data. It's a rough spot. I think it brings out how important a true backup strategy is. Backups and business continuity are not entirely the same thing all the time.

Hannan: That type of risk is so terrifying. It happened to one of our hospital clients recently. For them, they didn't have the time to roll back to backups to restore everything. They had to pay it because people's lives were at stake. It's terrifying.

Gibson: Phishing and ransomware are the big ones in the market right now. What's interesting though is they are really targeting small- and medium-size businesses. The big ones are getting hit and those are the ones you hear about. But it is the ones you don't hear about that concern me more because they aren't reported. They might not be in a regulated industry that requires them to report.

Smaller companies are targets because they may not have the resources to address some of these issues, such as employee training and awareness. Both ransomware and phishing come back to training and awareness.

Weber: Small business owners may not have a CIO or CTO. So how do they know if they are protected with cloud-based services or other tools out there?

Gibson: It comes back to what Michael and Tedrick said earlier. You've got to have policies in place. You've got to have a plan in place. But you have to be able to offer that same simplicity to your end users safely. So choose a platform, investigate it, and offer it to your employees so that they aren't going out and finding their own solutions to their problems.

Hargett: That's a good point. Security has to be something that protects your folks behind the scenes. If it's too hard, they're going to find ways around it. It has to be friendly.

Housh: I agree. In the old days, if you had a small- or a medium-size business, you would probably require two signatures for physical checks over a certain amount to make sure that it was something you actually wanted to go out.

The problem today is everything is so fast and electronic. You should have a procedure to cover your business in that same instance for wire transfers over a certain amount. You probably ought to verbally check any email request for that even though you're absolutely sure it's from the person you're talking about, because people are sitting and watching those email conversations. They are learning the nicknames and pets' names of the vendors and people with whom they communicate. I see email and wire transfer frauds every week.

It happens in all kinds of businesses, including professional services firms. Law firms have been victims of hacks, too. A couple of years ago, a law firm was hacked and information about a $40 billion merger among oil companies in Toronto was leaked.

I have a banking client who required that I have a two-number verification code on my phone to identify my phone for all of our conversations. With other clients, we don't just send emails back and forth. We go to a special place to exchange information, and it's not Google Docs or Dropbox.

Weber: I don't think we're ever going to stop having this conversation because as quickly as we can react, others are finding new ways to commit fraud. What other issues should we discuss?

Hargett: One area that is growing is network access control or device profiling. I think intelligent device profiling is an amazing tool. It allows you to see where network access requests are originating.

Housh: I think I should mention regulation. As we get ever more connected, it is going to get more difficult to transfer data across national boundaries. If you are doing business in Europe or anywhere across the world, or if you have a website open to people throughout the world and you get the data of an EU citizen, that citizen's country's laws will likely govern what happens to that data.

It's a worldwide web of risk, and the regulators—the FTC or the EU or anyone else—are all going to get their paws on it one way or the other and that includes attorneys general of the various states. It's something that you have to be cognizant of.

Gibson: I think the United States needs to come together under one, federal strategy. We've got all these different industries doing their own thing. To compete globally anymore, we really need to come to a conclusion on what the U.S. standard is for cybersecurity.

Weber: Cloud computing is often put forth as the panacea for security issues. Can companies rely on the cloud as a cybersecurity solution?

Gibson: I think the key there is delineating responsibility between the cloud providers and yourself—who is responsible for what.

Hannan: That is a great point. The vendor management piece is important. We're passing off risk to an outside party but that goes to the bigger picture of what cybersecurity is and even though we are passing the risk it doesn't mean that we can forget about it. It's not just cybersecurity. It's information security. We're passing off this risk because it's cheaper and easier. But how do you make sure that all vendors are doing what they are supposed to be doing? How are you monitoring your vendors?

Hargett: I agree with Jake. There are several "as a service" categories of service in cloud computing: infrastructure, platform and software, etc. And the line of delineation kind of moves within these different categories. So having that upfront knowledge before you start moving data into the cloud is key.

You have to continue to check with your provider. Ask about that life cycle management, whether it's from a software perspective or a hardware perspective.

Housh: I'm aware of situations in which people who had their backup information in the cloud had trouble retrieving it from their provider when an incident occurs. The cloud service has said, "Well, that information is mixed together with some other data and under our agreement, you don't have a right to that." That really stymies your ability to deal with the situation.

Running a tabletop simulation exercise with your incident group at your business would help identify these or other problems ahead of time.

Weber: That is key because those proactive steps are what keeps a lot of companies out of doomsday scenarios. It's always risk management. It's not risk-proof.