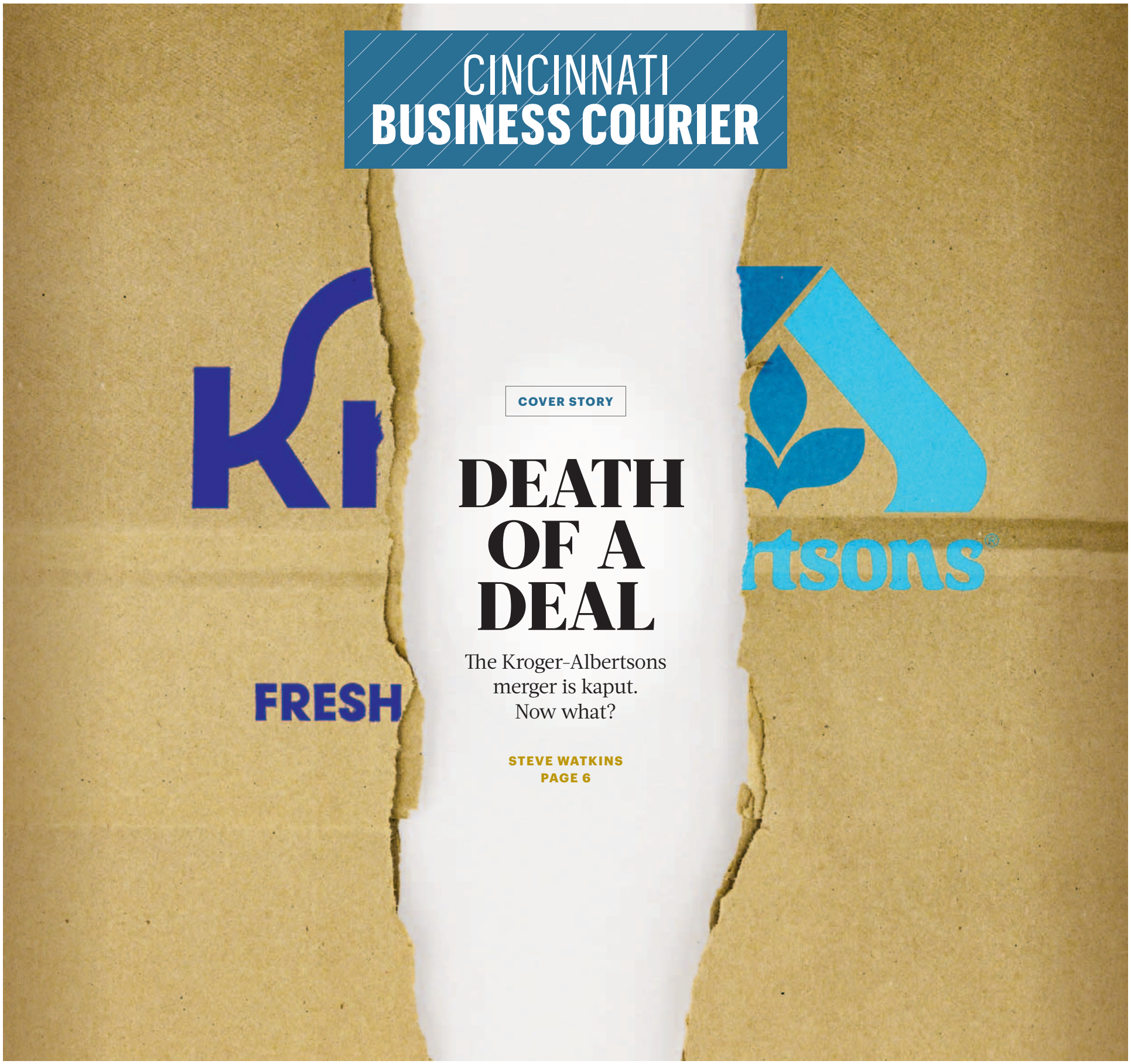
CINCINNATI
BUSINESS COURIER



COVER STORY

DEATH OF A DEAL

The Kroger-Albertsons merger is kaput. Now what?

STEVE WATKINS
PAGE 6

CORRIE SCHAFFELD | CBC

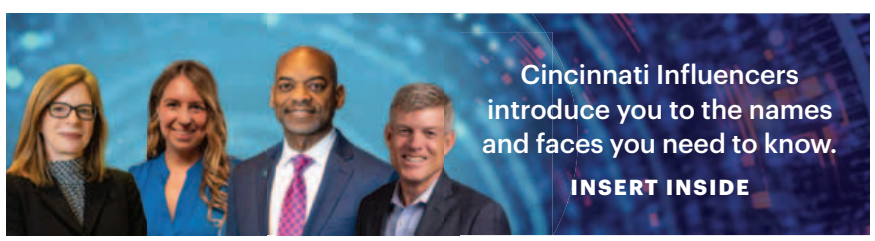


PHOTO BY: DAVID STEPHEN PHOTOGRAPHY

CYBER SECURITY FORUM

The growing cybersecurity threat:

What can be done to improve defenses

With a growing amount of personal, financial, health-related, and business-critical data stored and shared online, protecting this information from unauthorized access and theft is essential. Cyber threats are growing in sophistication and frequency, and no organization is immune from cyber-attacks such as hacking, phishing, ransomware, and malware. The Cincinnati Business Courier on December 4 presented a Cyber Security Forum that brought together leading experts who explored the trends, emerging threats, and best practices in cyber defense.

The panelists were: Joseph M. Callow, Jr., litigation partner and managing partner, Callow + Utter Law Group; Jesse Kegley, chief revenue officer, Emerge IT; and John Virden, chief information security officer and assistant vice president of security, compliance and risk management, Miami University. The forum was moderated by Jamie Smith, market president and publisher, Cincinnati Business Courier.

He began by asking about the biggest cybersecurity threats and trends the panelists see today. "Cybercrime is about to cost the world $10 trillion annually," he said. "That's a lot of money going to the bad guys." He cited AI and quantum computing as two trends to watch for. "The bad guys are going to use some of that $10 trillion and race to the technology that is going to enable them to be more successful at their nefarious acts," he said. "With AI, the lines are going to blur between: are we being attacked by a person or a machine? And what does that even mean?"

Virden said in the academic world and elsewhere, third-party vulnerabilities are a trend to be aware of. "I've heard, on average, some companies have about 1,000 third-party or cloud service entities that they will share data with," he said. "Last year at my university, we had 13 third-party vendors that experienced an

incident, and we have to track that, and monitor that, because we're responsible for that data that we gave." He said class-action lawsuits are also a concern post-incident. He also said the complexities of technology is a growing challenge.

Callow said he's found that two-thirds of data breaches are due to human error, such as being vulnerable to phishing. "The training of individuals and having people in touch with these issues is vital and important, because that's where it often happens." He said about 15% of problems are due to issues with vendors. He also mentioned customer portals, which allow customers to access invoices, upload ads, and do other work. "It's really important to know what barriers you put around that and determine who has access to that information," he said. "The more people who have access, the more potential you have for issues you'll have to deal with."

Kegley mentioned a recent client that had a key employee leave, and the small company had to reset 450 passwords. "You have a lot of different cloud applications, and each one has identity access and protection measures that need to be set up. So, the move to cloud, the move to integrate data between our businesses, all means that we have to secure differently," he said. He agreed that education about security, both in and out of the workplace, is essential. He also said he's seeing fatigue among business leaders in regard to cybersecurity because we are hearing about so many breaches. "There's so much noise that leaders don't know exactly what to do. They don't know where to start."

Virden added that identity access management is key. "That's what keeps track of the identities that you allow into your systems and what accesses you give them to get to those apps and portals," he said. "Somebody at your company should be thinking about that," he said. Miami has students, staff, faculty, former students, alumni, and retirees that it interacts with. He said starting by updating systems is important. "Modern systems are better and better at doing those protections, making sure you get the right folks access to the right information and the right systems at the right time."

Smith asked about any local incidents. Kegley said he recently worked with a midsized organization with a couple locations, and its VPN (virtual private network) wasn't protected. They experienced a cyber-attack that penetrated their network and accessed data. The client did not have detection capabilities or an incident response plan and was forced to pay ransom to have its network returned to service. He said cybersecurity needs to be seen as an ongoing program, not as a one-time project.

Callow said detection often begins when a senior executive can't access the system. "Those situations and how you react depends on how you prepare beforehand," he said. "The more things you've done beforehand, the better off you're able to handle an incident response," he said.

Smith asked about hybrid and remote work, with employees accessing data in public places and at home. Kegley said the focus has to be on user identity. "As data and applications move to the cloud, and people work outside of the network," he said, "you need to focus on identity. At the end of the day, it's making sure that you are who you are and only gaining access to the data that you're allowed to have access to."

From a legal perspective, Callow said his first thought is often about what information is protected by privilege and

THE PANELISTS

JOE CALLOW

Litigation Partner and Managing Partner at Callow
Callow + Utter Law Group

Joe Callow is a Litigation Partner and Managing Partner at Callow + Utter Law Group.

Joe has been advising clients and speaking about data privacy; data management; ediscovery best practices; and cybersecurity awareness for more than two decades. Joe helps write, review and update policies; advises on data breaches and cyber events; and educates clients, C-Suites, and employees on practices and procedures to minimize cybersecurity risk.

In his litigation practice Joe leads complex litigation matters on a national, regional, and local basis. He has over thirty years of experience in class action/ collective actions and multi-district litigation as well as environmental, antitrust, intellectual property, and general corporate/commercial litigation. He is a first chair trial counsel and has argued at the appellate level before the Ohio Supreme Court and multiple federal and state courts of appeal around the country.

JESSE KEGLEY

Chief Revenue Officer
Emerge IT

Jesse Kegley is a co-founder and Chief Revenue Officer (CRO) at Emerge, where he has been a key leader since 2007. A native of Northern Kentucky, Jesse began his tech career over two decades ago, initially helping a Kansas City start-up pioneer a cybersecurity detection service. At Emerge, Jesse drives Go-to-Market strategies, aligning with the company's growth-oriented core values. He also serves or has served on advisory boards for Cisco, Microsoft, and Ingram Micro, providing valuable insights into industry trends and technological advancements.

JOHN VIRDEN

Chief Information Security Officer (CISO) and Assistant Vice President of Security
Compliance and Risk Management, Miami University

John Virden is the Chief Information Security Officer (CISO) of Miami University and Assistant Vice President of Security, Compliance and Risk Management.

In these roles, he leads the information security program, manages strategic partnerships and orchestrates information security governance, risk-based direction, awareness, University consulting and cybersecurity operations. Additionally, he is a member of the Compliance Coordinating Council, the Information Technology Policy Committee, and the Institutional Response Team.

Virden has a wealth of information security experience and knowledge, most recently as the CISO at the University of California, Riverside. Along with his time in higher education, he spent a significant amount of his career serving in a variety of information and computer security positions within different facets of the US military.

what's going to get disclosed, assuming that litigation may be coming. "When an incident response happens and people start sending emails and saying things and describing responsibility, that all becomes potentially producible in litigation," he said. "The first thing I'm thinking about is controlling the information, trying to protect as much of it as privileged."

Virden said the university uses a risk-management approach to determine where to apply its resources. "Where's your sensitive data, where's the most sensitive data that needs to be protected with the most safeguards and what are most likely to be exploited?" he said. "That's where you want to focus your time and energy with the limited resources you may have." The university also has faculty who collaborate with people around the world. "So, we had to come up with a risk matrix so we could put those scarce resources to the right use," he said.

Smith asked, with threats evolving so quicky, how companies can stay up to date. Kegley said they should rely on trusted partners if they don't have the internal expertise to stay current. Legal assistance, insurance companies, and technology firms should be seen as partners. Online resources, information sharing and analysis centers can also help, he said. Sharing information among peer groups is especially helpful, he said. "Cybersecurity crime is a really big systemic problem, and it's affecting our community in ways that aren't always apparent," he said. "I encourage everybody to get with their peers and talk about it."

Virden added that connecting with law enforcement agencies is important. "Having a really good relationship in advance of the incident is key," he said. "If you're trying to get to know them during an incident, it's way too late." Callow noted that laws and regulations are a constantly changing landscape. "It is ever changing, and it's frankly overwhelming," he said.

Virden said the University follows a "compliance continuum," which comprises compliance requirements of all the industries it works with, laws and regulations and other provisions. The university takes those and builds standards, practices and guidelines, he said.

Smith asked about the legal profession and its use of artificial intelligence. The legal profession is one of the top three to five professions impacted by AI, Callow said. A recent study found that over 45% of what a lawyer does can be done by AI, he said. Document analysis and review is a leading area for the use of AI, as computers can review hundreds and thousands of documents far quicker than people can. "AI gives me the power to compete with larger firms that have more associates," he said. "It's a tool that's helpful, but you still have to put some parameters around it."

At universities, plagiarism is always an issue to watch for, Virden said, so faculty are wrestling with that now as some embrace AI, while others resist it. He cautioned that most information input into AI goes to the cloud unless you've created your own network, which some schools have done.

Kegley said AI is one of the largest technology inflection points of our time, but it comes with a lot of risk and concerns. Organizations need to decide on acceptable uses of it. As with any other new technology, businesses need to make sure they have systems to protect the organization before turning on functionality.

Smith then asked how individuals and companies should handle cybersecurity incidents. Kegley said organizations should have incident response plans, and exercise them, test them, and run different scenarios through it. "If you have a plan, but don't test that, you're not going to be prepared for it," he said.

Virden added that organizations should pick a framework for incident response. Miami uses an incident response plan developed by the National Institute of Standards and Technology. "We try to build our incident response plan around that," he said. Miami also does tabletop exercises at different levels of the institution. "We also do something that one of my guy's calls 'tiny tabletops.' He goes around different departments

and divisions and runs through about a 45-minute tabletop exercise. Then he usually gets another 45 minutes of questions."

Callow cautioned against letting CEOs negotiate ransoms with cyber criminals. "The reality is, you don't have a lot of leverage," he said. "It's not a typical negotiation. It's not a typical business setting, but lots of CEOs want to treat it that way, and honestly, I've never really seen it work out very well."

Kegley added that companies shouldn't be afraid to call their insurance providers about incidents or "events." "Every organization has a different risk profile but take a minute to understand what that risk is so that you can make an educated decision," he said.

Callow recommended using cyber incidents that are in the news as events to educate workers and remind people about company policies. Virden said businesses and others should "strive for a cyber security culture at their institution." He said that begins at the top. "You have to have leadership buy-in, and know that they get it, they understand it, and they demand that people think about cybersecurity, and protecting data." He also said it's important to tell employees that they must report phishing incidents or other problems when they happen. "They can't feel bad or embarrassed that it happened. It happens to all of us," he said. If someone gains access to the system, it may not be evident for weeks as the criminals search for vulnerabilities.

Smith then asked the audience for questions, and one member said his business was currently undergoing a ransomware incident. He asked why law enforcement wasn't taking the offensive against cybercrime. Virden said he's seen law enforcement temporarily stop a ransomware gang, but it' usually only temporary as the criminals reorganize. "It's global," he said. "The bad actors are all over the world, and law enforcement doesn't have the resources to address it." U.S. law enforcement agencies usually don't have the lawful authority to attack and search for bad actors, he said. Callow said it's difficult to track criminals in other countries. "A lot of it is foreign actors in foreign countries, and cells move, and cells change," he said. "That's why you stay up to date. It is not going to be stopped. It is not going to be resolved. If you resolve it with this group of actors, there are others that are going to fill that void."

Virden added that on average, 68 data-leak sites, a site that displays data that was stolen to the victims, show up every week globally. "If they want ransom, they're going to put it on their website and it has your name, your logo, a description of your company, and then it will have files that you can download that are unencrypted so you can look at it and say that's your company's data. That's 68 successful ransomware attacks that occur every week."

Kegley said organizations need to shift their mindset away from the physical and into the virtual because cybercrime can't be seen, unlike physical crime. Making information and systems secure enough to deter crime is important, he said. "Managing those safeguards, making sure that you're not vulnerable and easy pickings is a really good strategy," he said. "The initial reconnaissance is often automated, so they are able to identify vulnerability," he said.

Kegley closed by saying the terrain is evolving quickly and security demands more than just a one-time prevention. "This requires a program, not a project or single software tool that you can buy," he said. "It takes a combination of people, processes and technology to effectively mitigate risk."

Virden said practicing basics can go a long way. "Have strong, unique passwords for all your very important accounts. Don't share those passwords and use multi-factor authentication every chance you can. Back up your data and then practice restoring that data."

Callow said small businesses that don't have the resources that big ones do can still do the basics, such as changing passwords, limiting access and getting rid of data that's not needed. "There are steps you can take to at least make your situation better," he said.