[IN]SURANCE

Summer 2024

A publication of NAMIC®

INSIDE

FINDING THE RIGHT FIT

The current and incoming talent pools have the skills, but how do you assess if they're right for your company culture?

Q&A With Taft's Scot Ganow

WITH NEARLY 73 PERCENT OF ORGANIZATIONS GLOBALLY FALLING PREY TO A RANSOMWARE ATTACK IN 2023, THE PHRASE "WHEN, NOT IF" IS A VALID ONE. THUS, IT IS CRITICAL THAT COMPANIES TAKE EVERY PRECAUTION THEY CAN. IN MAGAZINE SPOKE WITH SCOT GANOW, CHAIR OF TAFT STETTINIUS & HOLLISTER'S PRIVACY AND DATA SECURITY PRACTICE, TO FIND OUT WHAT ACTIONS INSURERS SHOULD TAKE TO PROTECT THEIR INFORMATION.

Q: Tell IN magazine readers a little bit about yourself. How long have you been practicing as a privacy lawyer?

A: I have been practicing for nearly 15 years, but I like to share that I haven't always been a lawyer. If anything, it shows clients I have walked in their shoes. I worked in operations and management for health care and technology companies prior to assuming a role as privacy and ethics officer — yes, that gig is as cool as it sounds. This experience brings a sense of practicality to my practice. Any legal solution still must make operational and business sense to the client's business.

Q: Talk about what privacy and security lawyers do?

A: I like to say we do everything before and after a data breach. At Taft, we counsel clients in a proactive capacity. We assist with evaluating legal requirements, conducting risk assessments, developing policies and procedures to meet applicable data protection requirements, negotiating contracts, and helping with strategy on ways to leverage data more efficiently. We also help clients in a reactive capacity by responding to inquiries or complaints from data subjects or their counsel, guiding a client through an incident or data breach, and dealing with adverse parties when things go sideways.

Q: Malware, phishing, spoofing, ransomware, password attacks; there are so many threats out there. But what would you say is the greatest information security threat to companies?

A: I know people like to think it is hackers in hoodies. Because all hackers wear hoodies, right? But every year, surveys show employees are the root cause of most security incidents. While some employees act maliciously, even criminally, the majority who cause incidents are making mistakes or otherwise not complying with the entity's policies and procedures.

Q: Insurers, like all organizations, have numerous ways they can combat cyberattacks. But if there would be just one thing you would advise companies to do to help mitigate risk associated with information security, what would it be?

A: To be clear, there are no silver bullets to protect your data and systems. Rather, the most successful companies implement layered administrative, technical, and physical safeguards. That way, if one fails, the others will still protect the company. That said, one technical safeguard companies must implement is multi-factor authentication, which forces a user to

"Every year, surveys show employees are the root cause of most security incidents. While some employees act maliciously, even criminally, the majority who cause incidents are making mistakes or otherwise not complying with the entity's policies and procedures."

"There are no silver bullets to protect your data and systems. Rather, the most successful companies implement layered administrative, technical, and physical safeguards. That way, if one fails, the others will still protect the company."

provide a second code after providing a password to gain access to a system. Eighty-five percent of the breaches we managed last year would have been stopped if the client had turned on MFA. An administrative safeguard you must have is an employee training and awareness program to reach those very people who pose the greatest risk to your information security.

Q: You presented a session called "What I Wish Insurers Knew About Data Breaches" last year at the NAMIC Annual Convention. What were some insights you gave those who attended your session?

A: Combatting data breaches really takes a lot of time, energy, and money — all of which are not being spent on maintaining or growing your business. It takes even more time, energy, and money when you don't have the first clue about what data you have and where it is. Hence, the importance and value in doing your homework and diligence in advance by classifying your data, mapping the locations where you house such data, and identifying any applicable legal or security requirements.

I liken the importance of doing such data due diligence to following your doctor's instructions on dealing with heart attacks. If you were such a patient, what would you do? You would eat right, limit drinking, avoid smoking, and get regular exercise. Does this mean you will never have a heart attack? No, and the doctor would never promise that. But what medical professionals will tell you is that science shows those efforts help the patient survive the heart attack. That is the way you must look at data governance and security incidents. You will have an incident, but I can tell you from experience that companies that have done their diligence and data governance planning will more easily and successfully manage and survive such an incident than those that don't.

Q: What would you like readers to do in response to reading the insights you've shared?

A: When it comes to data governance and information security planning, just get started. To stick with the health theme, you will never be in shape on the first day of any workout plan. It could take weeks or months to notice results, but there is no question your health begins to improve the minute you start adopting healthier habits. Experts will tell you every little bit helps. The same is true with information security. Often, you don't have to outrun the bear, just the next company. Be a little more secure in your practices, and you'll be a little less attractive to hackers or less at risk of an employee error. Start with strong passwords and implementing MFA. Train your employees. Inventory your data and know where you keep it. It'll take some time to do so, but all serve to reduce the risks associated with information security. Just. Get. Started. [N]

"Combatting data breaches really takes a lot of time, energy, and money — all of which are not being spent on maintaining or growing your business. It takes even more time, energy, and money when you don't have the first clue about what data you have and where it is."