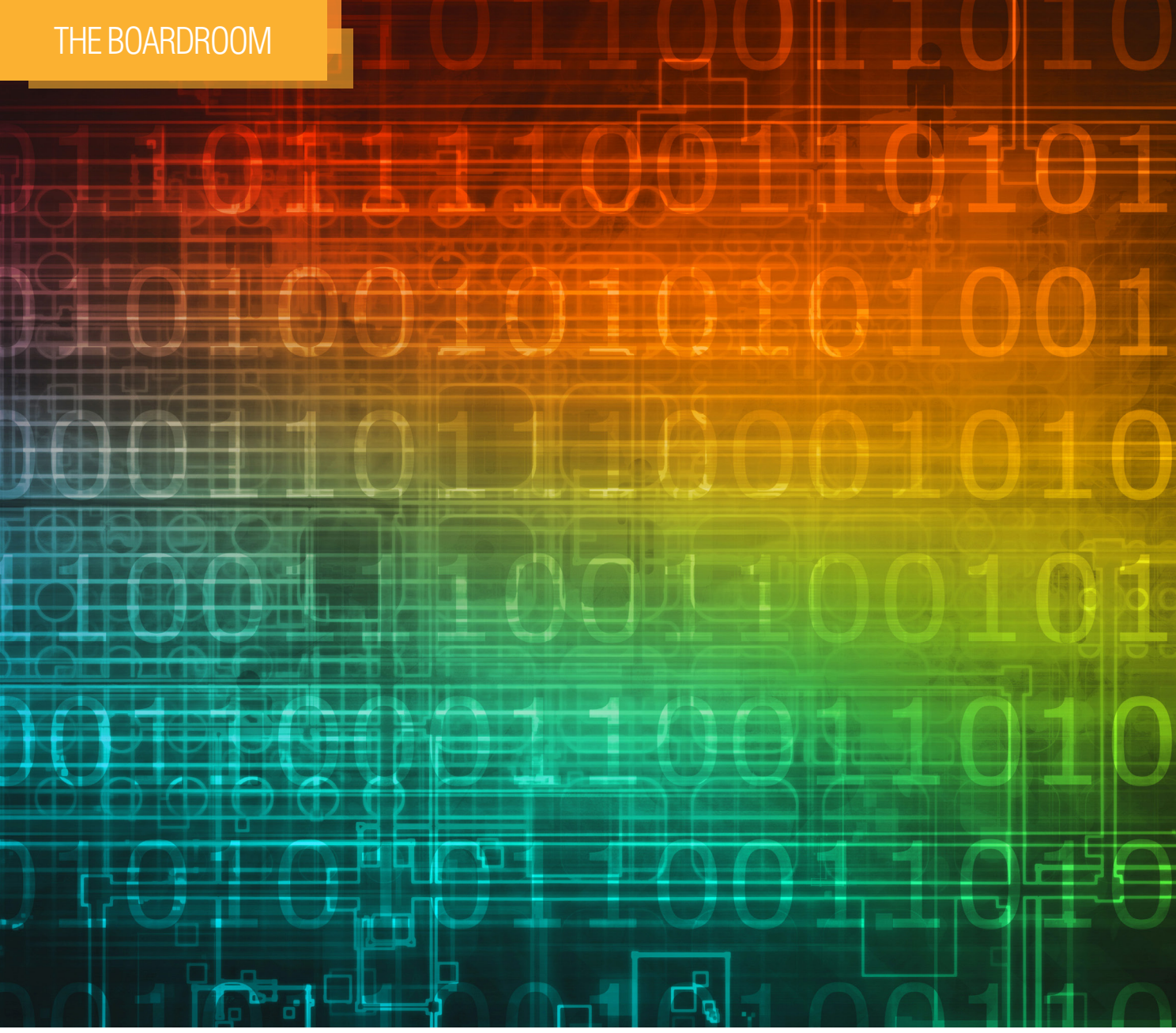


FILLING THE BREACH

Strong IT governance by the Board is a vital line of defense against cyber crime.

BY STACEY CLOSSER

Fill-in-the-blank Corp. confirmed today that hackers/ criminals/foreign agents/unauthorized users have accessed sensitive payment information/email addresses/business intelligence that may impact customers … Millions of cards affected … Working with law enforcement … Have enhanced our security protocols … Costs may adversely affect financial results …

The repetitive headlines and press releases remind directors that overseeing cyber security is one of the most pressing, and complicated, board responsibilities facing them today.

The cost of a data breach to a company can range from $9.3 million to $16 million, according to the *2014 Cost of Cyber Crime Study: United States,* the fifth annual study of U.S. companies conducted by the Poneman Institute. According to another Poneman Institute report, *2014 Cost of Data Breach Study: United States*, the average cost of each compromised

record caused by a data breach increased from $188 to $201 over the last year. Most of that money is spent on detection and recovery activities, followed by investigation and containment. Consequently, the longer it takes to resolve the breach, the more expensive it is.

It's a well-known issue — more than 65 percent of directors surveyed indicated that cyber security risks were at a high level or had increased, according to the Institute of Internal Auditors survey, "Pulse of the Profession 2014" — yet how to best provide oversight leaves some boards at a loss.

"It challenges each of us in our respective companies to have best practices," says Kneeland Youngblood, founding partner of Pharos Capital Group, who currently serves on the board of Mallinckrodt Pharmaceuticals and has also served on the boards of Burger King Corp., Gap Inc., and Starwood Hotels and Lodging, among others.

A BOARD'S RESPONSIBILITY

As part of their fiduciary responsibility, directors are charged with understanding the cyber risks against the organization as well as the legal implications. Boards ensure that the standards and processes followed by IT are rigorous and prudent, as outlined by external experts and measured against industry peers.

"IT IS IMPERATIVE THAT COMPANIES AND BOARDS BE VERY VIGILANT IN THEIR PEOPLE, IN THEIR PROCESSES, IN THEIR ASSESSMENT OF THINGS," SAYS YOUNGBLOOD. "TAKING THEIR EGO OUT AND ALWAYS STRIVING TO IMPROVE."

Once up to speed, the board should be performing an intensive review of the company's security policies annually, although those updates should occur more frequently during times of technological change or industry security upsets.

Youngblood outlines the first two lines of defense against cyber crime — having the right experience in the boardroom, and having the right experience in the management suite.

The most important thing the board of directors can and must do is to select the best CEO, says Youngblood. "All roads lead from there — if you get that right, many of these other things will be addressed."

The chief information officer is another important role that is best filled by looking at the marketplace, as opposed to an internal hire. The CIO position has evolved and now requires as much business acumen as technical know-how. This position won't be adequately filled by a tech genius lacking in social skills.

"The best CIO/CTOs can relate to boards and management. They know their business impact. They are not isolated, they don't talk in gibberish," says Tom Hudson, CEO of Municipal Parking Services and a serial entrepreneur who has served as a board member for numerous technology-related public and private companies. "They know the value that they are creating for the organization and the impact of a miss in money or time."

Robert Clyde, international vice president of ISACA (formerly Information Systems Audit and Control Association) and CEO of Adaptive Computing, underscores that sentiment regarding the CIO: "It's not enough to be a strong tech leader — you have to be a strong business leader." If the board determines the company CIO is the former, it might make sense to have the chief information security officer (CISO) report directly to the CEO or even the chief compliance officer "so you get a cross check on the security side," he says.

Providing the CISO access to the board is integral in keeping the lines of communication open. The board should expect to be made aware of attempted security breaches, not just the successful ones. Meetings with the CISO should reveal not only the appropriate strategy and possible roadblocks, but also the general risks facing the company's industry.

AREAS TO CONSIDER

Even seemingly non-IT business initiatives can be rife with security concerns. For example, outsourcing business processes such as accounting or human resources can provide an opportunity for cost savings, but it also introduces new cyber risk.

Third-party service providers' security practices quickly become your security practices. Boards should ensure that agreements with third-party providers address the provider's role in safeguarding critical data and require notification of any data breaches, while also applying those same requirements to

other third-party providers downstream.

The proliferation of "bring your own device" is changing the risk profile for organizations, says Clyde. Like it or not, employees will want to connect their devices to the network, and no amount of security awareness training will eliminate that behavior. The BYOD trend offers a "great competitive advantage, but you have to be sure to take care of the risks associated with that scenario," says Clyde.

QUESTIONS YOU WON'T THINK TO ASK

Board members don't need deep technical expertise to oversee cyber security, just the ability to read people and ask the right questions while staying out of the weeds of IT jargon. Stick to the basics: What, why, how, the results expected, and the process/investment required. Some other questions that may be off your radar include:

- Does management have established relationships with national and local authorities such as the FBI that respond to cyber crime? How can that relationship inform the company on security trends and new threats?
- How has the CEO communicated the importance of organizational security to all employees? Is there a security-awareness training program in place?
- Are we using a security framework such as NIST (www.nist.gov) or COBIT (www.isaca.org/cobit)

and is it up to date?

- How do our security measures stack up to our peers in our industry? What relationships can we leverage to find out?
- Big data offers opportunities to create very detailed customer profiles. How are we making sure that both the raw data and also those profiles are secure?
- Does internal audit have a direct line to the board's audit committee? "Most boards have those on the financial side, but there should be a similar avenue on IT controls," advises Clyde.

WHEN IT HAPPENS

All industries fall victim to cyber crime, albeit to different degrees. High-profile security breaches occur with such regularity that consumers have already registered data breach fatigue — more than one-third of consumers did nothing after being notified of a breach, according to research from Poneman Institute. But that doesn't mean organizations can, or should, be complacent.

Consider home security as an analogy: There are prudent, appropriate measures that should be taken — door and window locks, a security system, a dog, for example — but if a criminal is intent on getting in, there are ways to do it. That doesn't mean you give up and leave all the doors wide open, and it doesn't mean you go out and buy steel window covers that remain permanently closed.

Clyde encourages directors to ask: What are the right controls to have in place, given the assets we have and the likelihood of things occurring? What is the standard of due care for my industry?

"It is imperative that companies and boards be very vigilant in their people, in their processes, in their assessment of things," says Youngblood. "Taking their ego out and always striving to improve."

Industry experts agree that planning for a security breach is the best approach. It's not a matter of if, but when. "Any company can be hacked, it's really just a question of time and money of the attackers and how far they're willing to go," says Clyde.

When that happens, it's time to pull the trigger on the organization's detailed recovery plan.

"Be open and candid about the problem both internally and externally and put the right level of executive in charge of communicating about the crisis," says Hudson. "It probably did not get broken in a day and will take more than that to fix — plan for that."

DATA BREACHES: BY THE NUMBERS

COST OF A DATA BREACH TO A COMPANY CAN RANGE FROM

$$$$$$$$$$

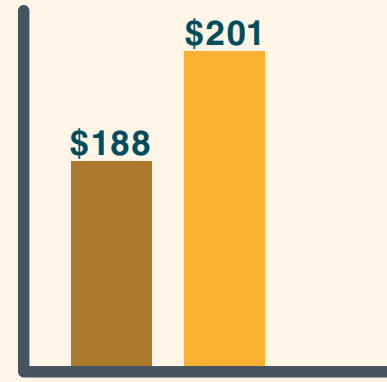
$9.3 MILLION

TO

$$$$$$$$$$$$$$$$$$$$

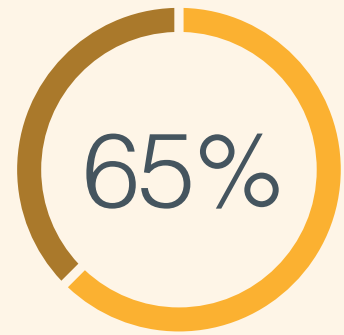
$16 MILLION

— 2014 COST OF CYBERCRIME STUDY: UNITED STATES



AVERAGE COST OF EACH COMPROMISED RECORD CAUSED BY A DATA BREACH INCREASED FROM $188 TO $201 OVER THE LAST YEAR.

— 2014 COST OF CYBERCRIME STUDY: UNITED STATES



MORE THAN SIXTY-FIVE PERCENT OF DIRECTORS SURVEYED INDICATED THAT CYBER SECURITY RISKS WERE AT A HIGH LEVEL OR HAD INCREASED.

— INSTITUTE OF INTERNAL AUDITORS SURVEY "PULSE OF THE PROFESSION 2014"