Board Leadership

January–February 2026 • No. 203

Innovative Approaches to Governance

EDITOR: NICHOLAS KING

Newsletter Article

You Have Been Hacked—Now What

By Rick Williams

Rick Williams is a leadership expert and founder and managing director of Boston-based consulting firm Williams Advisory Partners. In this article, he discusses cybersecurity and the board's role in responding to cyberattacks.

Ed Murphy is CEO of Happy Rack, a regional retail chain based in Chicago. He and his leadership team opened their weekly 8 AM Zoom call on Dec. 15. As they started to review November performance and preparation for the final weeks of the Christmas season, they could not share their files.

Ed asked Helene, the IT director, to check why the company's servers were not responding. Helene tried shutting down and restarting one of the servers and then saw other issues. She quickly realized that the servers had been hacked. Helene recommended to Ed that they shut down all company servers and computers as quickly as possible. With the names changed, this is the story of a real cyberattack and the takeaway lessons for company leaders and boards of directors.

What to Do Now?

When Ed Murphy realized that most of the company's files were frozen and inaccessible, thoughts of what to do raced through his mind. Call the police. Call the board. Contact customers. Contact the press. Contact shareholders. Contact employees. Re-read the cyberattack response plan. His thoughts bounced across a complex matrix of responsibilities and liabilities for the company, his staff, and the board.

Ed realized that the first question he will be asked is, "*what will you do about your customer's private data?*" The second question will be, "*what did you do to prevent the attack from happening?*"

Today's Reality

Hacks and data breaches have become a persistent part of life in the 21st century, and the proof is in the news. Ransomware has crippled towns and cities. Hackers have penetrated the cyber defenses of most companies, including many smaller companies, often without the company knowing it. In today's reality, every company must have a cyber defense plan:

- Assume you will be attacked.
- Identify your most valuable digital assets.
- Prepare to defend those assets vigorously.
- Assume your defenses will be breached to some degree.
- Prepare a breach reaction plan.

Theft of physical assets, embezzlement, and shoplifting are business realities. Cyber threats challenge a company across several new dimensions: lost IP (intellectual property), lost private customer information, lost private employee data, and possible violations of data protection regulations. Data fundamental to the company's continued operations can be locked up or lost.

These losses can result in lost reputation, customer confidence, and brand value. Companies are responsible for protecting private information under their control: patient data, personal data, customer financial information, customer credit

continued on page 2

Inside This Issue

HACKED

continued from page 1

cards, etc. Failure to protect this information exposes the company and, in some cases, board directors and officers to financial liabilities.

Hackers stole credit card data for 40 million Target customers. North Korea stole movies and confidential communications from Sony Pictures because the government did not like its portrayal in the movie *The Interview*. Russian operatives stole personnel files from the US Office of Personnel Management for 18 million current and former federal employees. Verizon reduced its purchase price for Yahoo by $350 million after it had a massive data loss.

T-Mobile lost control over millions of people's personal information, Apple releases one software update after another to plug security holes, and Twitch had all of its source code—along with information about streamers' pay—leaked.

These mega cyber breaches are in the headlines. But cyberattacks are an everyday and largely unreported reality for virtually every company in the US and much of the world. Phishing attacks attempting to gain access to your network are pervasive. The Better Business Bureau warned small businesses against opening an email with the Subject*: QuickBooks Support: Change Request*. A link in the email downloaded malware that gave hackers full access to the company's network, including passwords.

Hackers got access to Target's credit card data through an HVAC contractor in Pennsylvania with malware on its network. The contractor maintained Target's heating and cooling systems. Using the malware, the hackers stole the contractor's password for access to the Target network. Once inside and using a bona fide password, there were no barriers to the hacker from accessing Target's highly confidential customer information.

Symantec reports that half of large companies have significant breaches each year, and one quarter of smaller companies are breached. The cost of responding to each of these breaches is about $15 million for larger companies and $4 million for medium-size companies, according to the Ponemon Institute. Small business costs are about $700,000 per incident, forcing many smaller companies to close.

The *Wall Street Journal* profiled the attack on Houston-based United Structures of America. Following an earlier virus attack, the company president, Dain Drake, upgraded the IT system with an up-to-date cyber defense hardware. After a second attack that locked the company's files, Dain discovered that the security system had been installed but was never tested and was ineffective. Even after paying a ransom, the company did not recover all of its data and filed for bankruptcy.

The movement toward open platforms and widely shared data across the company, combined with laptops, phones, and tablets connecting to the network, has increased transparency and productivity. But these changes also make the network more vulnerable. Most organizations have moved to remote work for at least some operations. Laptop computers at home and other insecure locations opened new channels for cyber breaches and lax cyber defense.

Cyber criminals see smaller businesses as a less-prepared target. According to surveys by RiskRecom, a Mastercard company, breaches at smaller companies have jumped twice as fast as larger company breaches. Disgruntled current employees who sell data to other hackers or take the data or IP to their next employer or a foreign government are a real vulnerability.

Individuals in the US and abroad will attempt to hack into your network, but they are not as dangerous as organized or sponsored attackers. Theft of digital information using sophisticated technology and long-term persistence is undertaken mostly by:

- Criminal gangs in Russia and Eastern Europe.
  - Selling the data on the black market.
- Demanding ransom payments to unlock files.
- Chinese government organizations
  - Capturing IP for domestic use

Negotiating with the Attacker

When Ed Murphy and his senior leadership logged into their computers and onto the company network, a "worm" spread to their computers and servers linked to them. A Read

continued on page 6

BOARD LEADERSHIP

BOARD LEADERSHIP: INNOVATIVE APPROACHES TO GOVERNANCE (Online ISSN: 1542-7862) is published bimonthly by Wiley Periodicals LLC, 111 River St., Hoboken, NJ 07030-5774 USA.

Wiley's Corporate Citizenship initiative seeks to address the environmental, social, economic, and ethical challenges faced in our business and which are important to our diverse stakeholder groups. Since launching the initiative, we have focused on sharing our content with those in need, enhancing community philanthropy, reducing our carbon impact, creating global guidelines and best practicesfor paper use, establishing a vendor code of ethics, and engaging our colleagues and other stakeholders in our efforts. Follow our progress at www.wiley.com/go/citizenship.

Editor: Nicholas King. **Publishing Editor:** Samara E. Kuehne. **Production Editor:** Shriya Upadhyaya. **Editorial Correspondence:** nicholaskingllc@gmail.com.

Policy Governance is a registered service mark of John Carver.

For submission instructions, subscription and all other information visit: wileyonlinelibrary.com/journal/bl

View this journal online at wileyonlinelibrary.com/journal/bl

WILEY

WINNER 2024 APEX AWARDS FOR PUBLICATION EXCELLENCE AWARD OF EXCELLENCE, NEWSLETTERS

HACKED

continued from page 2

Me message came up saying that the files were encrypted. The attacker included a contact link to regain access to the files.

Helene shut down some computers and servers before the Happy Rack staff connected to the network, but the worm was blocking most company files two weeks before Christmas. That Friday morning, Ed had to decide what to do. Some backup files were at his home, but they were dated and incomplete.

Ed pulled advice from his team and then called his attorney. "Don't contact the attacker," was the first recommendation. Helene suggested reaching out to Unit 42, a cybersecurity consultant based in Palo Alto, CA. They became the company's point of contact with the attacker and worked with Happy Rack's IT staff trying to recover the blocked files.

Ed contacted the FBI. Beyond a recommendation not to pay a ransom, the FBI and local law enforcement were not helpful.

The attacker demanded $2 million to unlock Happy Rack's files to be paid in bitcoins. Over eight high-stress days, Ed Murphy negotiated with the attacker through Unit 42. The attacker had access to some of the company's financial files and had estimated what they believed Happy Rack could pay. Understanding what the company could pay and what the attacker thought it could pay was part of the analysis.

Ed asked whether they would recover the files even if they paid the ransom. Unit 42 told Ed that this attacker had a reputation for doing what they said they would do. Unit 42 required the attacker to demonstrate that they could unlock some of the encrypted files.

Ed must choose. Pay a significant ransom to regain access to the company data and files or try to reconstruct the data over many months. Fair or unfair, right or wrong, was not the question. Laws and law enforcement of criminal activity were not engaged to help Ed and Happy Rack.

Happy Rack is a privately owned company with about $120 million annual revenues. Ed did not have the complication of public shareholders, but confidential customer and vendor data were at risk. Ed's dad founded the company and was a key advisor as Ed made the essential decisions. The attacker seemed to have access mostly to public data about the company's financial condition. They did not have as much access to confidential financial data as originally feared.

In the context of the company's financial capability and what the company could pay, the original ransom demand was lower than it might have been. Ed negotiated a payment for accessing the files at about half the original $2 million demand. Unit 42 received the encryption key to review. With Unit 42's assurance that the key would work, Ed authorized the ransom payment.

The encryption key worked, but many files were corrupted requiring cleanup. The company did not have insurance covering ransom payments, but insurance covered the $500,000 in legal fees. Ed believes that someone inside the company clicked on a link in a phishing attack, bringing the attacker into the company. But, Unit 42 could not determine the source of the breach with certainty.

While Ed responded to the cyberattack, he also kept the company's operations going without access to essential files and data. I asked Ed how he made the difficult decisions that brought the company through the crisis. He looked to his professional advisors, including his attorney and Unit 42 for their recommendations. The company CFO and his dad became the core advisors helping him make the most important decisions. The company has a board of directors, but, as a family-owned business, the board was not the decision-maker.

Prepare to Be Attacked—Your Cyber Defense Plan

Start with the assumption that you will be attacked. You probably have been attacked and perhaps penetrated.

A cyberattack is an attack. Your primary vulnerability is usually not a direct assault on your network but an indirect attack. Entry into your networks will come through an employee or outside vendor. Sixty percent of cybersecurity attacks come through third parties. Vendors, contractors, employees, and others routinely connecting to your network are the primary risk category.

Every company has a different risk profile. Use these best-practice questions and recommendations as a starting point for developing or reviewing your cyber defense plan.

1. What is authentically important to protect?
   Focus on how data are handled and protected—customer, financial, IP, operational.
   Operating systems are less important.
2. What are the channels of vulnerability to your most important data and files?
   What vendors and contractors have access to your network?
   What can they access?
   What vendor equipment is connected to the network?
   Which employees have access to what?
3. Isolate valuable assets on high-security networks separated from other networks.
   Only accessible by company-approved devices.
   Only accessible by approved employees.

4. Ensure that monitoring systems are in place to detect attacks and breaches.

   Monitor for cyber breaches in real time.

   Larger companies should engage consultants to attack their defenses and find vulnerabilities.

5. Back up critical data and isolate it from attack.

   Prepare to bring critical systems back online after the attack.

   Keep software on networks, work stations, and desktops up to date with cyber protection updates.

   Consider the advantages and liabilities of putting data in the cloud.

6. Prepare employees to protect the company's network and assets, training, awareness, scouts for danger.

7. Plan for when an attack occurs.

   Who will be notified?

   Who will decide to initiate the cybersecurity plan?

   Who will decide next steps?

   Who will speak for the company, and what will they say?

Defending against cyberattacks is a difficult challenge. There are not many apparent pathways into the company and no simple defenses. Every organization with more than a few employees has many digital channels into its data networks. Vulnerable pathways include thumb drives picked up in the parking lot, employee emails connected to the internet, service contractor's links into the company, subcontractor components connected to the company's network, stolen laptops, and theft by faithless employees. With persistence, bad actors can access to the company's systems and assets.

Too often, cybersecurity is seen as a specialized technical issue to be managed by the IT department. The potential for financial and reputational loss from a cyberattack is so large that delegating cyber defense strategy to the IT department is no longer a viable or responsible approach. Every part of the organization—from the board room to the shipping room—has a role in defending the company.

Vendors and contractors with access to your networks are high-risk channels into the company. Isolating their access to limited segments of your network is the first step. Requiring that they certify their cybersecurity status is the next. Your vendors and contractors will have contractors and vendors to them with exposure risks difficult for you to evaluate and manage.

Your circumstances, the risks involved, and your relationship with the contractors will determine whether you require verification of the contractor's security status and the status of their contractors. Trust but verify is the required approach.

Most cyber breaches begin with an employee clicking on a link or downloading a file without understanding or realizing they are launching an attack on the company's assets. Employee training is essential, but it should be directed at developing values, attitudes, and routine cyber practices that protect the organization's digital assets.

Response to an Attack

First order of business—don't Panic! In some cases, hackers will steal data, and you will not know it was stolen. In time, you hear that your customer data are for sale on a website used by Russian hackers. As in the Happy Rack case, hackers can encrypt the company's files and demand a ransom to unlock them.

After you discover a breach or learn an attack is underway, your primary responsibilities are:

- Minimize further damage to customers, employees, or patients whose private information was captured.
- Secure access to the company's physical and IP assets.
- Restore company operations.
- Discover the source of the breach and close it.
- Inform law enforcement—FBI, state attorney general, SEC.
- Speak with one voice to the public, customers, employees, and investors.

The reality of today's world is that an attacked company must discover how the bad guys broke in and close the breach. But the company cannot be fully open about the investigation's progress and results. Outsiders will ask about compliance with federal and state requirements for an Information Security Plan covering the data inventory, security for the data, and data disposal. Plaintiff attorneys will use this information to claim that the company had not reasonably protected the compromised data. The contention will be that the company should have anticipated the attack and prepared adequate defenses to safeguard the private data.

If your company is attacked, you must launch public and private responses immediately. Legal, ethical, and public expectations are high. Without a plan in place before the attack, the chances are high for missteps, misstatements, and higher legal and financial liabilities and reputational losses.

Steps You Can Take

Most companies today are underprotected and do not understand their vulnerabilities. As the company CEO or board of directors, here are steps you can take to limit cyber risks and reduce the company's financial and reputational liability.

1. Cybersecurity is an important corporate risk management issue for most companies. Make core funding and priority decisions at the board and CEO levels.

2. Be sure that the company's cybersecurity plan identifies high-value assets and their vulnerability to cyber theft. Develop a plan to protect these specific risks—avoid, accept, mitigate, or transfer the risk through insurance. Develop a second plan to manage lower-value assets.

3. Make smart investments in cybersecurity by understanding the unique risks of your organization and the cost/benefit trade-offs of the realistic options available.

4. The board and other senior leaders, not just the IT department, should periodically review the adequacy of defenses, employee training, and real-time monitoring with the assistance of inside and outside cybersecurity experts.

5. Don't allow your company's cybersecurity to depend on the security of vendor's software over which you have no control.

6. Ask if cyber defenses are adequate and if outside testing is needed. If the answers to these questions are Yes and No, ask for a justification for these answers.

7. Be certain the company has followed the federal and state requirements for an Information Security Program and an Incident Response Plan. A Security Programs Team Leader may also be required.

8. Develop a culture of cyber awareness through training and messaging about the role of every employee in defending the organization.

9. Prepare for the breach—who decides what and who speaks.

If you are the company's leader or its board of directors, you are expected to put in place policies and procedures that protect the company, its employees, its customers, and its assets against cyberattack. *Your real responsibility is to be sure that these procedures actually work.* ■

Rick Williams is an inspiring speaker and author sharing his insights and experience as a company founder, CEO, scientist, management consultant, and board member. Rick speaks about "*Making Difficult Decisions*" drawing on his acclaimed leadership guidebook, *Create the Future*. Williams engages with an international audience through his newsletter with 50,000 readers, published thought leadership articles, and speaking engagements for leadership audiences. For more information, visit https://rickwilliamsleadership.com.

News and Updates

Bloomerang Webinar Gives Tips on Board Fundraising Techniques

Bloomerang is hosting an on-demand webinar titled "Ditch the gala: Board fundraising with equity and impact" on its website.

According to organizers, this webinar is for those looking to shake up their traditional board fundraising programs. Nonprofit board members attendees this webinar will discover new tools to build authentic donor relationships, elevate community voices, and promote inclusive, values-driven giving. They will leave energized with practical strategies to drive meaningful impact and transform fundraising approaches, organizers said.

More specifically, the webinar will:

- Identify and address inequities in fundraising.
- Engage diverse donors authentically and purposefully.
- Center equity in board fundraising strategies.

This webinar is being offered free to the public.

For more information, visit https://bit.ly/3MjWcKJ. ■

Blueavocado.com Webinar Offers Training on Nonprofit Governance Basics

Blueavocado.org is hosting an on-demand webinar titled Nonprofit Governance Training 101 on its website.

The webinar draws from a live Q&A session from June 12, 2025, that discussed the essential governance topics like board structure, legal compliance, and best practices.

As organizers note, running a nonprofit is challenging on many fronts and good governance is essential for long-term success.

To that end, this webinar engages all levels of nonprofit leadership and management—including board members, executive directors and department leaders and key staff—looking to boost their organization's impact.

Led by panelists Casey Williams, Partner and Chair of Liebert Cassidy Whitmore's Nonprofit Practice, and Anni Safarloo, Associate at Liebert Cassidy Whitmore, the webinar will go over what every nonprofit needs to know and dive into the essentials of nonprofit governance.

Topics covered include:

- Board structure and composition.
- Key policies and best practices.
- Legal compliance and financial oversight.
- Common challenges and how to overcome them.
- The legal and ethical responsibilities of nonprofit board members.

This webinar is being offered free to the public.

For more information, visit https://bit.ly/4ryz4bE. ■