# PROTECTING

SPECIAL ADVERTISING SECTION

# WHAT COMPANIES NEED TO KNOW TO PROTECT THEMSELVES FROM CYBERATTACKS

**Cybersecurity has become increasingly important as more products and services leverage the Internet to improve functionality, expand availability and increase connectivity. But as companies become more integrated with the Internet, so does the risk of a cyberattack or security breach. The Milwaukee Business Journal recently assembled a panel of experts to explore what companies – large and small – need to know about cybersecurity today.**

**MODERATOR:** WHAT THREE THINGS SHOULD EVERY COMPANY, REGARDLESS OF SIZE, THINK ABOUT REGARDING CYBERSECURITY?

**JEFF OLEJNIK:** First, you have to understand what "crown jewels" you are protecting. It could be financial accounts, patient records, intellectual property or perhaps logistics information. Second, you have to identify and manage your risk. What are your vulnerabilities and how are you managing them? Are your employees trained and do you have appropriate preventive safeguards in place like perimeter protection, software updates, access and authentication? There are always new vulnerabilities for attackers to exploit.

**JOE HEINO:** It's not a question of whether a company will be attacked – it's a question of when. That's why every company should understand what a cyberattack is, where cyberattacks can come from, and how cyberattacks are best managed.

**NATHAN LASNOSKI:** Companies need an executive-level security program that is transparent, organized, and prepared. It cannot be "hidden" within IT, since it impacts the very reputation of the organization, its customer data, and its financial well-being. The program needs to be organized, leveraging a modern framework like NIST Cybersecurity Framework (CSF). And the program needs to be prepared to the extent the company has prioritized and mitigated its key "blocking and tackling" risks and reduced its attack surface. Being prepared also means having an effective secu-

***"A company with even moderate technology usage would suffer a substantial reputation and financial impact as a result of a successful breach."***

**NATHAN LASNOSKI,** Concurrency

## TABLE of EXPERTS

**JOE HEINO**
*Davis & Kuelthau*
Joe is a registered U.S. Patent Attorney and a Shareholder at Davis & Kuelthau. He represents a wide range of regional and national clients in the manufacturing and service sectors in all areas of intellectual property law, including patent, trademark, copyright, and trade secrets, as well as licensing and franchising. Joe helps businesses build fences around their IP, allowing them to maintain technological and market advantages over their competitors throughout the world and in cyberspace.

**NATHAN LASNOSKI**
*Concurrency*
Nathan is the Chief Technology Officer at Concurrency, a national technology solutions company headquartered in Brookfield, WI. He is responsible for helping customers realize the value of Digital Transformation through an inventive set of integrated technology consulting services. Nathan is responsible for what Concurrency delivers, how it is delivered, and the operational delivery of technology services.

**JEFF OLEJNIK**
*Wipfli*
Jeff Olejnik is a highly-experience IT security professional and Director in Wipfli LLP's risk advisory services practice. With more than 20 years in the industry, Jeff helps clients manage risk through effective information security, business continuity planning, and program management. He is a seasoned entrepreneur with proven experience in building successful companies in the IT services industry.

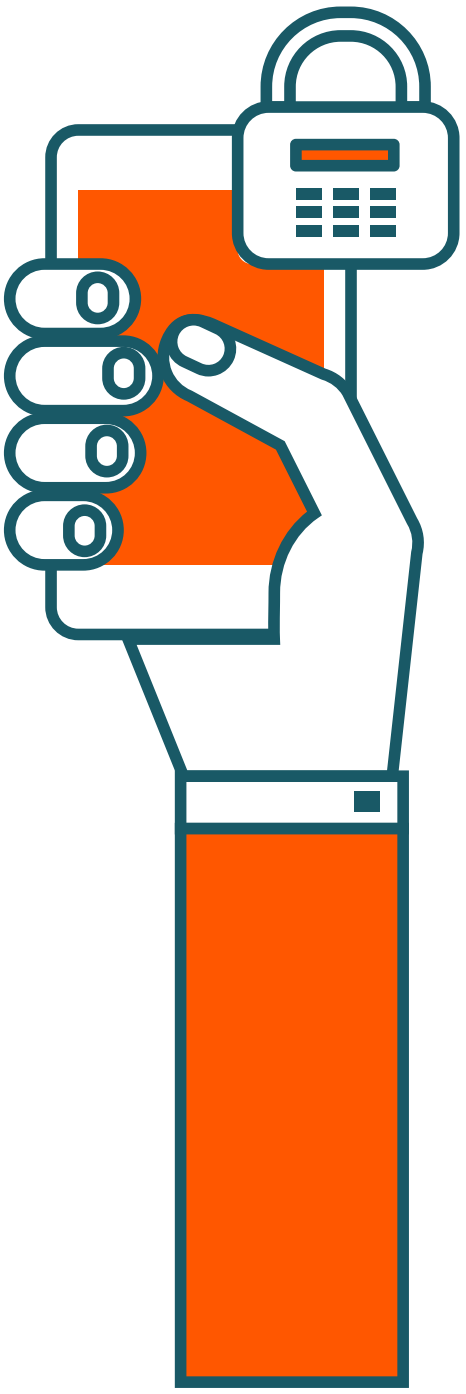
# YOUR PERIMETER

SPECIAL ADVERTISING SECTION

rity incident response process, proactive work management processes and security management tooling.

MODERATOR: WITH EVERY DATA BREACH, THERE IS A LOT OF DISCUSSION ABOUT ITS IMPACT ON PEOPLE. THE EQUIFAX DATA BREACH, FOR EXAMPLE, IMPACTED OVER 145 MILLION UNITED STATES CITIZENS. HOW DO THESE BREACHES IMPACT BUSINESSES?

**OLEJNIK:** Because of all of the personal identification information compromised in the Equifax breach, it will be important for businesses to take extra precautions to verify identities when opening accounts, extending credit or hiring employees. Companies will also face increased scrutiny from clients and prospects about how they are managing their cybersecurity risks.



**LASNOSKI:** A company with even moderate technology usage would suffer a substantial reputation and financial impact as a result of a successful breach. The impact grows as the products delivered to the organization's customers increasingly leverage technology.

**HEINO:** From a law firm perspective, a good example of a breach is the DLA Piper cyberattack in June of this year. DLA Piper is a mega-firm with offices in over 40 countries. The firm's initial assessment was that the attack was ransomware, which is a cyberattack that holds files hostage for a fee. It was later learned that the attack was wiper ware, an attack that destroys files altogether. The attack forced the firm to shut down its digital operations around the world. Attorneys within the firm conducted business by using personal cell phones. Trial attorneys were denied access to key documents and transactional attorneys were unable to close deals. The effect of this attack on the firm's clients will likely never be fully assessed.

MODERATOR: IN LARGER COMPANIES, HOW CAN SENIOR MANAGEMENT BE CONFIDENT THAT ITS CYBERSECURITY PROGRAM AND CONTINGENCY PLANS ARE ROBUST, EFFECTIVE AND IN COMPLIANCE WITH BEST-PRACTICE STANDARDS AND BREACH NOTIFICATION LAWS?

**HEINO:** Senior management must establish and maintain relationships with federal, state and local law enforcement and other related regulatory agencies that deal with cyberattacks. This includes having an ongoing program to expose management to agency members who are aware of current and anticipated attack trends.

**LASNOSKI:** Management needs to evaluate if its security program is consistently leveraging an enterprise framework such, as NIST CSF, and is regularly tracking proactive and operational backlogs. Many companies have security programs, but they are often not managed practically or are hidden from the executive team.

**OLEJNIK:** In order to exercise adequate oversight, senior management and boards should be asking questions like: Where are our top cyber risks? How are we managing these risks? What would we do if we had a data breach or business interruption

today? Companies can find out a lot about organizational preparedness by going through tabletop exercises that simulate a company's response to a breach.

> ***"Small companies need to be even more diligent in efforts to prevent ransomware attacks, because they are prime targets for such attacks."***
>
> **JOE HEINO,**
> **Davis & Kuelthau**

MODERATOR: WHAT CAN SMALLER COMPANIES DO, ESPECIALLY IF THEY LACK DEDICATED STAFF AND HAVE LIMITED FINANCIAL RESOURCES?

**OLEJNIK:** For companies that don't know where to start or have a limited budget, I recommend securing the Internet perimeter. This is the digital door into your network and must be secure. Hire a company to do some external vulnerability assessment or penetration testing. Train your employees. You can have the world's best technical solution, but it takes just one click on a link or a lost, unencrypted laptop to create a major incident. Teach employees how to protect themselves and your business. Finally, use good security hygiene. Patch and update your systems, back up your data, use complex passwords, and limit administrator privileges so that employees cannot download malware or unapproved software.

**HEINO:** Small company owners and management need to stay aware of current and anticipated attack trends. A good resource is the Federal Trade Commission's annual "Privacy and Data Security Update." Even small companies should have a response team. Unfortunately, small companies need to be even more diligent in efforts to prevent ransomware attacks, because they are prime targets for such attacks.

**LASNOSKI:** Companies large and small must deal with a scarcity of resources. The challenge for both is managing that scarcity and applying it to the most relevant risks. This can be made more effective by using a major framework, using an agile backlog to prioritize mitigation into practical sprints, and using a clear operational process. The effectiveness of a security program is directly related to whether a company has an effective structure for managing it.

MODERATOR: WHAT ARE THE CRITICAL COMPONENTS OF A BUSINESS CONTINUATION PLAN AND WHO SHOULD BE INVOLVED IN PUTTING THAT PLAN TOGETHER?

**HEINO:** A business continuation plan requires that the company identify and prioritize its most time-sensitive business activities, determine what resources are needed to fulfill continuity requirements, and conduct a risk assessment to limit the impact an attack would have on key business activities. In order to do this, IT and management need to work together.

**OLEJNIK:** Successful business continuity plans require executive support and sponsorship, typically from a C-level executive. The planning process should identify the recovery and availability requirements for every area of the organization. The business needs to identify tolerance for downtime and data loss in every area. Then, IT needs to be heavily involved in implementing and documenting the necessary recovery steps. Most importantly, they need to practice simulated breaches and test their responses.

**LASNOSKI:** A recovery plan that isn't tested isn't worth much. The most effective technologies and plans allow for validation in virtual environments that don't negatively affect production. A plan also needs to be comprehensive, at least in the extent to which it aligns to organizational priorities. Finally, a plan needs to be structured so that a service can be recovered independent of another service. This is increasingly important with the cloud, since recoveries will be more service-centric.

MODERATOR: HOW IMPORTANT IS VENDOR MANAGEMENT IN TERMS OF CYBERSECURITY? WHAT CAN COMPANIES DO TO ENSURE THEIR VENDORS' CYBERSECURITY IS SUFFICIENT FOR THE DATA THEY ARE HANDLING?

**LASNOSKI:** Any effective security program needs to include controls for customers, partners, and employees since they all have the potential to negatively impact the overall security of the organization, as well as each other. The technology for better integrating partners is starting to evolve, allowing for more fine-grained controls, auditing, just-in-time access and content control.

**OLEJNIK:** First, classify your vendors. Vendors need greater scrutiny if they have access to confidential information or are critical to your operations. Identify the minimum expectations for security controls and communicate the expectations to your vendor or prospective vendors. Have them attest to whether or not they meet the expectations. If they don't, have a conversation to discuss compensating controls or action plans. You should also review results from their independent audits, such as SOC 2 reports.

**HEINO:** A good place to start is to work with vendors who are familiar with the "Critical Security Controls" that have been established by the Center for Internet Security. The most important controls include the creation of a device inventory, requiring secure configuration for all devices, conducting security skills assessment and training, and instituting vulnerability assessments.

MODERATOR: WHAT ARE THE BENEFITS AND RISKS OF USING CLOUD STORAGE AND/OR CLOUD-BASED APPLICATIONS?

**OLEJNIK:** In general, cloud service providers can offer solutions capabilities that would be cost prohibitive for many businesses; however, companies that adopt cloud services need to develop the skills necessary to manage outsourced relationships.

**HEINO:** On one hand, cloud environments provide the ability for vast amounts of data to be stored on cloud servers. On the other hand, cloud providers are an attractive target based on volume alone. Further, while cloud providers may deploy security controls to protect their environments, cloud users are ultimately responsible for protecting their own data in the cloud. The Cloud Security Alliance has recommended that cloud users use multifactor authentication and encryption to protect against data breaches.

***"Another emerging issue is the labor shortage. The demand for cybersecurity skills is greater than the supply."***

**JEFF OLEJNIK,**
Wipfli

**LASNOSKI:** The use of cloud-based applications absolutely changes the architectural and operational model for the delivery of secure technology. It is both a risk, due to the new knowledge necessary, and a benefit, due to more complete and modern security capabilities. The responsibility of a business leveraging the cloud is to understand that operationalization of the environment is as important as launching the cloud service. It cannot be an afterthought.

MODERATOR: WHAT ARE SOME OF THE KEY CYBERSECURITY RISKS ASSOCIATED WITH MOBILE WORKFORCES? DO THEY VARY DEPENDING ON THE SIZE OF THE EMPLOYER?

**HEINO:** The obvious risk is not the mobility of the workforce, but the mobility of the devices used by the workforce. In order to ensure that client information is not accessed via a lost device, a "poison pill" can be installed in or sent to such device. This feature allows the lost or stolen device to be disabled, thereby preventing access to secure client data.

**LASNOSKI:** A mobile workforce accentuates many of the cybersecurity risks that already exist in a business and remind us that the models for controlling access, data, and reputation are managed differently. The modern workplace also causes identity to become the new control mechanism.

MODERATOR: HOW DOES A COMPANY CREATE A CULTURE THAT ENSURES EFFECTIVE CYBERSECURITY WITHOUT HARMING PRODUCTIVITY OR EMPLOYEE PARTICIPATION?

**OLEJNIK:** People need to think of security policies and controls as guardrails instead of roadblocks. They are in place to keep the car on the road, not to prevent the car from moving forward. That's the message that needs to be reinforced by management. If people understand why they need to have long passwords that need to be changed every 90 days, they generally are more accepting of the policy.

**HEINO:** Unfortunately, cyberattacks are the new norm and they present themselves in many different forms. The company's internal culture needs to accept this as a new reality so that everyone's "radar" is up. That is much more productive than having to divert resources when a data breach occurs. Employees need to understand that breach investigations and customer notifications can rack up significant costs. Further, the loss of business from an attack can adversely impact a company for many years after the attack.

**LASNOSKI:** The key to deploying effective cybersecurity is to make it reasonable. If an organization is too draconian, employees will work around the corporate standard. Having reasonable methods will result in more compliance and better security controls.

MODERATOR: SECURITY RISKS AND THEIR IMPACT ON BUSINESS CONTINUATION ARE CONTINUALLY EVOLVING. WHAT ARE SOME OF THE 'WHAT'S COMING NEXT' ISSUES THAT COMPANIES NEED TO BE THINKING ABOUT AND PLANNING FOR?

**OLEJNIK:** Securing the Internet-of-Things devices. Internet-enabled products like refrigerators, cars, baby monitors and insulin pumps become new attack targets for cybercriminals. Security needs to be included in product design and QA testing. Another emerging issue is the labor shortage. The demand for cybersecurity skills is greater than the supply. Many companies will either need to review their compensation plans relative to market demands or consider outsourcing cybersecurity services to specialists.

**LASNOSKI:** As companies infuse technology into their business models they need to consider how security and business continuity factor into that sphere. Ultimately, every company is becoming a technology company and this necessitates that appropriate controls be integrated into the company's offerings to mitigate risks and deliver a quality product.

**HEINO:** Honestly, no one knows what is coming next, which is why business continuity plans need to be fluid and adaptable. In the legal arena, this is somewhat similar to the "dot com" explosion, where it has been difficult for legal solutions to keep up with business realities. This is how cybersecurity will continue to be.