VULCAN.

What is cyber negligence and how can we avoid it?

As cyberattacks grow in volume, sophistication and magnitude, headlines advise caution and echo calls for heightened protection.

These attacks are agnostic – attacking organizations with fortified systems and ample security resources as well as smaller, more volatile companies. It is therefore understandable that a “victim mindset” has set in, generating significant fear and a sense that impending attacks are unavoidable. While it is impossible to obstruct every possible security risk, a more useful framework for security professionals to consider is viewing these risks through a “negligence” lens. The following commentary on cyber negligence and how to avoid it was taken from Ryan Gurney’s keynote presentation at the Remediation Summit, in November, 2021.

Don't be a cyber victim

A "victim" mindset can lead to feelings of helplessness, generating a crippling response by security professionals who view attacks as inevitable and fatal. Choosing to become reactive rather than proactive, this attitude may lead security leaders to choose mediocre protection for all assets, without conducting strategic assessments as to what data is most sensitive and where their focus should be.

Negligence is defined as failing to take the steps a reasonable person might take in a similar situation. Everyone is negligent on occasion—sending a text while driving, leaving the kids in the car when you run in to grab something at the convenience store, opening a suspicious email link. These are common actions that may be categorized as negligent once something does go wrong. Reasonable people avoid negligent activities the vast majority of the time.

A perfect storm of increased threats targeting unmitigated vulnerabilities, under-resourced teams, and a resulting crush of unrelenting work has pushed the cyber security industry to the brink of negligence. A negligent approach may relieve some of the pressure on cyber security professionals, as avoiding the most likely risks and taking reasonable precautions is a straightforward, but limited approach to security. It may not eliminate all potential risks, but it gives you a good sense of where to start and how to approach "reasonable" risk assessment. This might work some of the time, but organizations can quickly learn first-hand the shortcomings of such an approach.

2014

Sony hack

A case in point is the 2014 cyber attack against Sony, which occurred several months after its release of “The Interview,” a satire based on the North Korean dictator. The attack resulted in personal data, emails, business information and other highly sensitive information being leaked and malware attempts perpetrated, as attackers demanded the cancellation of the film. Sony employees noted the attack had sent them “back to the Stone Age.” While that might be an exaggeration, it did send them back to the “paper ages,”’ as they temporarily reverted to using fax machines and handwritten notes to communicate. The connection between the movie’s arguably controversial subject matter and viewpoint was understandably linked to the attack; had Sony’s cybersecurity team considered the possible repercussions during filming and release?

Again, it’s speculative to say North Korea initiated this attack, but it does prompt the questions, “Which companies are prepared to withstand an attack by a nation-state? Under what circumstances should a company expect a cyberattack by a nation-state?” And considering current events, it would be negligent today to not consider nation-state sponsored cyberattacks.

Censorship of political commentary would be tragic for freedom and democracy. At the same time, in releasing this type of film, it would be negligent to ignore the possibility that the North Korean state might take action in response. Whether that action may include a cyber attack or a public relations attack cannot be anticipated—but a top-tier media company such as Sony, releasing contentious content definitely incurs some level of risk, cyber risk included.

Paperwork doesn't mask negligence

One common way companies have been handling security and compliance risk is by "outsourcing" it. For example, when companies use cloud computing services, the agreements may include highly detailed clauses regarding the security precautions the cloud service will provide.

Similarly, a partnership in which companies exchange intellectual property may include various clauses about the liability that one company has in respect to the other. Pages of questionnaires are sent back and forth between vendors, supposedly to ensure security controls are in place.

Based on a growing accumulation of cyber risk documentation and paperwork, organizations may feel secure in terms of legal liability and compliance. Unfortunately, no signed document or agreement does anything to actually deter cyber attacks. What truly matters are the actions taken by each of the parties in terms of the actual technology implementation, not the service level agreements or legal declarations.

You can tell the paperwork has taken over when the vendor or supplier agreements contain clauses that are obviously unlikely to be executed. Such clauses will include words like "always," "every," and "immediate." Real-world examples include requirements such as, "Customer must review all background checks for any persons with access to customer data." And, "Customer must pre-authorize all access to data." It is simply not reasonable to expect those types of clauses to be implemented.

Therefore, organizations should consider getting the legal and sales teams out of the room when the security officers and technical team meet. Rather than discussing compliance and covering up any potential liabilities, the security team can go through the actual risks and the IT team can define technical steps they are taking to mitigate, remediate and secure their organization against real breaches. Obviously, the lawyers can get their questionnaires answered and documents signed at the appropriate juncture, but no reasonable person would consider the documents to be a substitute for the cybersecurity solutions that need to be implemented.

Negligence and real liability

Legal liability is a small part of the picture. Compliance and legal responsibility come into play on a regular basis in regular audits and in companies' attempts to avoid fines for compliance breaches. However, a compliance breach is not a security breach.

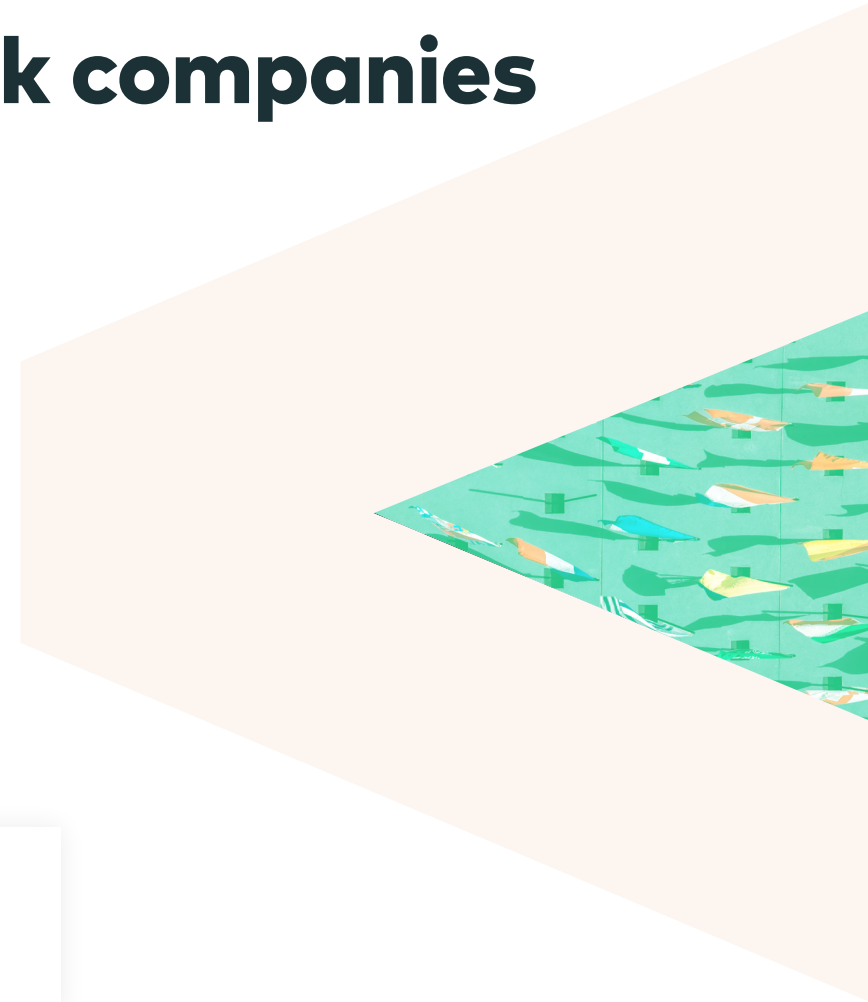
Real liability takes two forms:

1 Data security: When it comes to data security breaches it's essential to take all of the standard precautions as well as the appropriate steps based on the company's risk profile.

2 Damage to the company's image: When it comes to company image and public relations, avoiding negligence is essential. Even if a breach does occur, if the team has taken reasonable precautions, the damage—both material and reputational—will be reduced.

In major cyber attacks that hit multiple companies, the public relations damage to any specific company is reduced as it is distributed across many entities, which means it's even more essential to be less negligent than the other hacked organizations. While a security breach causes real damage, you can avoid compounding that damage into a public relations issue if you've followed the negligence-avoidance principle.

Why nation-states attack companies



While the Sony example above may seem extreme, many industries today fall into categories that can be of interest to powers at the nation-state level. Some examples are obvious, such as financial services, energy, infrastructure, media, and health technologies. Others are less attractive to attackers, but because some countries have strong ties between government and industry, simply competing with a foreign country may be enough to garner some level of government-sanctioned cyber intervention.

When assessing the security risk in any given situation, companies should take into consideration the following factors:

- Culture
- Industry
- Products
- Data gathered and stored
- Data-gathering techniques
- Customer profiles
- Community interaction
- Activism
- Media and publicity

Each of these areas carries with it specific risks that need to be addressed as cyber risks.

Staying above the negligence bar

Regardless of risk, there are some basics that every company needs to have in place. The internet is full of automated bots and crawlers that scan for common vulnerabilities such as unpatched software, insecure passwords, and unassuming people who will simply click on suspicious links. To stay above the negligence bar, companies need to take care of the following security basics:

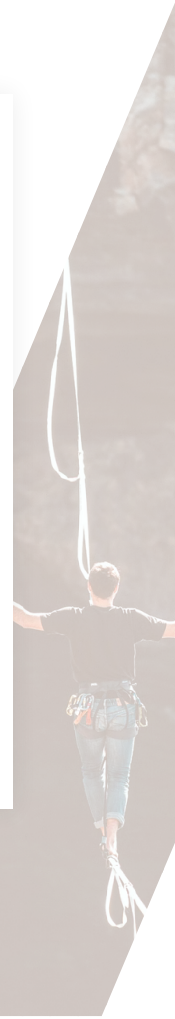
- Access controls
- 2FA/MFA and password managers
- Encryption and proper key management
- Malware protection
- Security monitoring and risk management
- Security training
- Third-party assessments and audits

Finally, most companies will want to consider having an appropriate security framework in place. There are several common frameworks that companies can refer to, such as CIS Critical Security Controls.

Keeping it basic:

Averting the risks of being the weakest link

Start by addressing known but unmitigated vulnerabilities such as cloud misconfigurations and unpatched software. The vast majority of cyberattacks occur due to basic negligence, as hacker probes are constantly seeking targets. It doesn't matter if you have the best lock for your bicycle, as long as it's better than the one on the bicycle next to yours. If you have the basics covered, these probes will find another victim before they get to your company.



True cybersecurity risk assessment

One of the clauses included in some vendor security agreements is, “Vendor must remediate all known vulnerabilities within 24 hours.” It sounds good on paper, but represents a misunderstanding of what cybersecurity actually entails.

Risks fall into different categories in terms of the number and types of users they will affect (employees versus clients), the amount of data that is exposed, the type of threat in terms of the consequences, and so on.

Today, security scans and artificial intelligence systems are available to surface the risks that are truly in need of immediate attention. The security staff needs to be constantly vigilant in terms of assessing and addressing the risk, but the job of risk identification can be automated to a large degree.

Don't pass the buck

Another danger of compliance documentation and vendor agreements is that it can give a company the false sense of control and security. As a security professional, make sure that you are involved and clear about the measures your partners and vendors are taking. Leaving the agreements to the lawyers may leave you exposed.

While the compliance and legal agreements may be in place, without speaking to your peers at partner organizations, you may never know if they are structured to implement the security elements within these agreements. At the end of the day, you're going to be held responsible, so look into any activities being performed on your company's behalf.

Prioritized security risk control

Security risks are a part of business operations, and can't all be managed at all times. The intelligent way to approach risk is to identify the urgent and serious risks, the risk that could potentially have the most impact to your business, and to handle those before dealing with insignificant risks. Any business environment with digital infrastructure at scale is practically impossible to monitor for all risks at all times. Therefore, it's important to implement security solutions that scan the systems constantly and prioritize risks, not just list them.

Prioritized security risk control is the methodology companies use to constantly eliminate the highest risks for the organization.

The first step is using automated security scanning and identification software to prioritize and repair the most urgent vulnerabilities across the entire organization. This type of risk control factors into the company's strategic goals and specific assessments of the risks associated with the company's activity.

Once a company has identified the risks based on their products, markets, customers, etc., that information can be configured into a security risk control model which can provide specific risk control recommendations based on the company's specific profile.

These types of solutions can provide comprehensive and straightforward reports that show the tangible results of security activities being performed.

Prioritized risk control takes organizations from borderline negligent, to proactive mitigation of the likeliest risks and provides protection with a level of security that everyone across the organization can appreciate.

This content is based on The Remediation Summit keynote address titled, "Be Better Than Negligent," by Ryan Gurney, CISO-in-Residence at YL Ventures.

Get full ownership of your cyber risk across all your attack surfaces. Go beyond vulnerability scan data with powerful risk prioritization, orchestration, and mitigation capabilities of Vulcan Cyber®.

About Vulcan Cyber

Vulcan Cyber® breaks down organizational cyber risk into measurable, manageable processes to help security teams go beyond their scan data and actually reduce risk. With powerful prioritization, orchestration and mitigation capabilities, the Vulcan Cyber risk management SaaS platform provides clear solutions to help manage risk effectively. Vulcan enhances teams' existing cyber environments by connecting with all the tools they already use, supporting every stage of the cyber security lifecycle across cloud, IT and application attack surfaces. The unique capability of the Vulcan Cyber platform has garnered Vulcan recognition as a 2019 Gartner Cool Vendor and as a 2020 RSA Conference Innovation Sandbox finalist.

Start owning your risk

TRY VULCAN FREE