The changing nature of security in 2021

INFORMATION SECURITY FOR ENTERTAINMENT ADVISORS

T/A

TRUSTED ADVISOR

Supported by:

MILLER KAPLAN

Q3 2021

Table of Contents

The evolution of ransomware Information security is a topic that finds itself in a unique position in the collective mind of the public. On the one hand, if you were to take a poll on the importance of information security, the results would be resoundingly in favor of placing a high priority on protecting information. However, most companies readily admit that they are not prepared in the case of a cyberattack.

> **“ Never before in the history of humankind have people across the world been subjected to extortion on a massive scale as they are today**
>
> - Symantec, The Evolution of Ransomware

The problem with securing information is that it can seem too big to tackle—and because of this, many choose to avoid it altogether. Some may be naïve; others may be lazy. Many more will trust that the latest software loaded onto their computer will keep them secure. It is 2021, after all. But while we expect our software to be secure in the modern age, hackers have and always will be one step ahead. Not only that, but as we’ve seen recently in the news, it seems that many software and hardware providers aren’t doing the right thing with regard to protecting the software that they sell you.

Bringing your business up to speed with modern cybersecurity practices and putting policies in place might initially appear to be a massive undertaking. With a subject as vitally important as information security, responsible companies need to do more than trust that IT has everything under control because it is highly likely that your IT department has not been fully trained in this discipline.

But with the proper guidance, any company, large or small, can build an information security strategy that enables secure business. While you can never be too secure, there is also a level at which you can responsibly keep your information safe without breaking the budget.

“It’s important to note that practicing information security is not about being 100% secure; it’s about protecting yourself at a commercially reasonable level.” – David Lam, CISSP, CPP; Partner & CISO Miller Kaplan

Ransomware Accelerates to Critical Mass

With increasing velocity over the past ten years, ransomware recently hit peak public awareness when Colonial Pipeline, one of the largest oil pipelines in the United States, was held hostage by a hacker group known as DarkSide.

Weeks later, the largest meat manufacturer in the world was targeted by a sophisticated ransomware attack. And similarly, they had no choice but to acquiesce to the attacker’s demands. In 2021, those demands have predominantly been payment in Bitcoin.

Colonial Pipeline was forced to pay $4.4 billion worth of Bitcoin to reclaim control of its systems. In 2020, close to $350 million worth of cryptocurrency was paid out in ransomware attacks, up 300 percent over 2019. Bitcoin allows the attackers to be paid efficiently, and more importantly, anonymously.

The First Known Ransomware Attack
Ransomware might seem to be a relatively new phenomenon, but the first known ransomware attack dates to 1989. While this first attack used floppy disks armed with a Trojan, modern ransomware is much more cunning and infinitely more dangerous. Modern ransomware truly took off in 2011, as close to 60,000 new cases were detected in the third quarter of 2011 alone. That number doubled by the third quarter of 2012, and by 2015, there were over 700,000 detected cases of ransomware.

What Is Ransomware?
Ransomware is when a company’s computer systems are hijacked using encryption so that you cannot access your data, and to regain control, the company must meet the hijackers’ demands.

According to Axios, “Today’s ransomware world operates like a macabre parody of the modern tech industry. The original backers, the ‘venture capitalists’ in the equation, are governments looking to ‘disrupt’ their enemies. These investors pay

third-party hacking groups who function as 'entrepreneurs' and 'startups.' Their products are technical platforms that enable 'users' to launch ransomware attacks, producing a revenue stream."

What Is the Difference Between Malware and Ransomware?

As David Lam described to the Los Angeles times, "Whereas typical malware steals your data, ransomware renders your systems unusable, which is the worst of nightmares."

Once the attackers have infiltrated, the entirety of your systems and data have now been taken hostage. When this happens, a company has little choice but to comply with the ransom demands.

Biggest Cybersecurity Risk
The most considerable risk your company can take regarding cybersecurity is to be underprepared—or worse, not prepared at all. According to Ian C. Ballon, Co-Chair, Global Intellectual Property & Technology Practice Group, "One of the greatest threats is a lack of preparation. Most businesses should assume that they will experience security incidents despite their best efforts. But if they plan ahead, they can mitigate the impact of an incident."

When a ransomware attack strikes, you are left with access to nothing. To potentially have the entirety of your company's data wiped from existence is a terrifying prospect. After realizing the severity of a ransomware aftershock, the question goes from "should we prepare?" to "how much should we prepare?"

Are Small Businesses Targets for Ransomware?
"Data assets are the most valuable – and vulnerable – components of the global economy." – Varonis

When we see a dominant oil pipeline in the United States and the largest meat producer in the world both get shut down by ransomware attacks, it would be human to think, "well, that won't happen to my small business." However, while the headlines are dominated by the jaw-dropping scale of ransomware at the highest level, that does not mean small businesses are immune to this type of attack.

As of 2019, 60 percent of small companies went out of business in the first six months after falling victim to a cyberattack or breach. More significantly, firms with famous clients will be

targeted at a much more significant rate than other businesses due to the leverage provided by controlling their data.

How Should a Company Prepare for a Cyber Attack?

"We cannot stop attackers from wanting to breach our defenses, and there is no way to account for all possible modes of attacks." – Chant Vartanian

These preceding words by Chant Vartanian to the Los Angeles Times are cold but accurate. And the sooner a company realizes this reality, the sooner they can begin to defend themselves in a commercially reasonable manner. Vartanian goes on to say, "cyber defense will always be reactive, and it is safe to assume the bad actors are always one step ahead."

Again, organizations must realize these cold hard facts before they can fully move forward with an information security strategy. To defend against this cruel reality, a company can deploy multi-layered security protocols with the ability to detect an attack in its early stages.

As David Lam wrote for Forbes, there are seven things you should be doing to protect your organization from a cyberattack:

1. Information security policies and standards must be in place. Setting standards and policies is step one, no matter who you are or how large or small your company is. Information security policies and standards form the framework of your entire information security strategy.

2. If you can, get cybersecurity insurance. Cybersecurity insurance is still a burgeoning industry, and your coverage can vary significantly from one plan to another. However, you may never feel happier to have insurance if you do suffer a breach. So, investigate cybersecurity insurance further for your needs.

3. Once your program is in place, pay attention to the basics. Most organizations are infiltrated by a phishing attack or from a drive-by (browsing the web and clicking a malicious link). Once this simple mistake has been made, the hacker can take over that computer with admin privileges. This happens most commonly when a system has not applied the proper patches. Unfortunately, many companies rely on automatic patching. But without a vulnerability scanner, hackers will take advantage of the cracks in the system.

4. Remember that your people are your critical assets, and they must be trained continually. This means going beyond online training only and forming small groups of 10-13 people. At a bare minimum, your highest-level officials should be rehearsing what they will do in the case of a breach.

5. Part of your training should ensure that your people know how to report suspicious events. One of the most significant factors in limiting the damage of a cyberattack is how quickly it is reported. If you can catch a breach in the early stages, you can reduce the damage done. Also, if a user reports a potential cyberattack in the first few minutes, exposure can be greatly limited.

6. Vet your vendors. According to Lam, "many vendors do not have even minimal commercially reasonable information security practices in place." Such as those policies and standards mentioned at tip No. 1. Most

> **"Many vendors do not have even minimal commercially reasonable information security practices in place.**
>
> - David Lam, CISSP, CPP;
> Partner & CISO Miller Kaplan

critically, if you are using that vendor, especially if they service your IT needs, you are placing your company at significant risk.

7. Ensure that your IT vendor or IT department is applying commercially reasonable tools to secure your network. An example of a commercially reasonable tool is an intrusion detection system (IDS). What an IDS would catch, for example, are signatures left by an intruder.

"Since tech is so heavily entrenched in our culture, its vigilance is imperative. There is no one-stop solution to address this requirement. However, we need to implement multiple layers of security that can alert us early." – Chant Vartanian

Lam concludes his Forbes article saying:

"Remember that information security is not reliant on just one layer. It's important to have multiple layers of protection, known as defense-in-depth, to protect your systems. That's why selecting the best tools you can afford, from both a time and money perspective, is an important step in the protection of your organization. Information security is not a destination – it's a journey."

The Challenge of Information Security in Remote Work Environments

"The biggest threat we see from people working at home is the catastrophic misunderstanding that you can safely use a personal machine to access corporate networks without substantial information security in place." – David Lam

One way companies can combat the challenge of securely working in remote environments is to "use technology to enforce that only authorized machines can access your systems." This tip comes from Miller Kaplan Chief Information Security Officer David Lam in a social engineering article for Forbes.

Lam also suggests always using multifactor authentication and conducting ongoing training and awareness for potential phishing campaigns. He also explains the importance of having an incident response and communications plan. "It's important to have a plan in place before something bad happens, so you know what to do and how you are going to communicate with your stakeholders."

"The digital landscape is going through a reformation. With the workforce moving to remote, we are facing a unique challenge of keeping tabs on data movement." – Chant Vartanian, Chief Strategy Officer, M-Theory

Continuous Training is Critical
"There is nothing called 'too much security.'" – Chant Vartanian

In a Los Angeles Times feature on modern cybersecurity, the experts were all in agreement that a lack of preparation is the kiss of death when it comes to surviving a cyber-attack.

"It is important to plan ahead," said Ian C. Ballon. "I have repre-

> **“The number one thing you can do to strengthen your cybersecurity is to implement an Information Security Management Program.**
>
> - David Lam, CISSP, CPP;
> Partner & CISO Miller Kaplan

sented companies in connection with cybersecurity breaches going back to the late 1990s – before notification laws made disclosure mandatory in certain cases when companies treated security breaches like property losses – and the one common theme is that businesses that haven’t planned ahead are more likely to make mistakes.”

The training required is not always high-level. The first step should be ensuring that your employees are well-trained in noticing the signs of a common attack. According to Vartanian, “regular training for users on best practices to follow and how to identify malicious content goes a long way.”

At a minimum, the key components of your company that coordinate together during a cyber-attack should have periodic training sessions to simulate an attack. These components include a company’s CISO (chief information security officer), public relations, and legal. If a company does not have a CISO, this role should be filled by a senior executive supported by subject matter expertise.

While no amount of training can fully prepare you for a cyberattack, imagine how it would play out with zero training whatsoever. Even if a company does employ a CISO, according to ZDNet, “under half of CISOs are ready to respond to a cyberattack.”

This is a troubling statistic, but one that rings true when listening to industry experts. There is a severe lack of security talent and expertise available. This again highlights the importance of continually educating and training your staff—especially those at the C-level.

Information Security Management Program (ISMP)

An information security management program is a means for an organization to follow the appropriate security standards and policies necessary to stay secure. Lam explains, “this gives you the bar that you need to meet and a methodology for meeting that bar.” Lam elaborates, saying, “the goal of this program is to operationally manage information risk. From there, everything is dictated by your management methodology as defined in the ISMP.”

In other words, once you have your systems and policies in place and have checks and balances to govern your information, it all boils down to following a methodology. And in this case, the methodology should already be pre-determined by your independent advisor.

According to Lam, for a small company with three or four IT personnel, much of what you need to set up the proper business framework can be found in Office 365. It then becomes a matter of knowing how to take full advantage of the tools at your disposal. “In the current business world, phenomenal security tools are already there,” Lam continued, “And people just don’t know.”

Additionally, companies with a solid set of security systems and policies can:

- **Lower cost on infrastructure.**
- **Lower cost of IT support.**
- **Make the claim that the company’s information security is “commercially reasonable.”**

Lam elaborates, saying, “you are looking to bring all that together holistically. The idea is to get down that road strategically and safely. And really have an optimized IT experience. If you know the right questions to ask, you can get there relatively quickly.”

While getting your company to a more secure state and setting the proper standards may not take as much time as you fear, establishing a protected information security network is a long-term vision, not a short-term fix. As Lam states, “we say, ‘How do we make life better? It’s not just locking down [your information]. It’s about enabling business in a secure way.”

Commercially reasonable is a legal term that means that the actions taken by your company regarding information security are considered reasonable, good faith efforts. This distinction can be important when explaining a breach to a client or defending yourself against litigation. What it means for your information security to be commercially reasonable will vary for every company, depending on its size, the amount of data that needs protecting, and the contents of that data.

Lam concludes, “If you approach this from the long-term strategy, and you look from a process-oriented perspective, you can build these scalable tools at really reasonable costs. And the payback is fast.”

Data Backup and Antivirus Protection

“When it comes to protecting data, antivirus and backup work together to combat a wider range of threats than either one of them working alone can prevent.” – Muhi Majoub, Chief Product Officer, OpenText

Antivirus protection and backing up your data might come off as an automatic no-brainer to some, or these tasks may appear as an unnecessary annoyance to others. At the most basic level, these are two of the most critical basic hygiene investments you can make. No one ever wants to go to backup, but not having a backup can be a business ending event.

Backup and antivirus software that comes preloaded onto your computer is a only a start, To be effective, your backups and anti-malware protection must be enterprise grade. This doesn’t have to cost a lot, and should be implemented in consultation with subject matter experts. And, if you aren’t testing your backups, it’s almost as good as not having them. According to Lam, “We’ve seen so many companies not be able to get their data back because their backups weren’t working properly or didn’t backup the right information. Testing is cheap insurance against this horrible outcome.”

How should business managers set up information security standards?

"Business management firms are some of the most vulnerable in this space. Specifically, because they have all this data, for all these people, with all this money." – David Lam, CISSP, CPP; Partner & CISO Miller Kaplan

To properly secure your company's data, it is recommended that you consult with outside help. Unless your company already employs a Chief Information Security Officer (CISO) and utilizes a robust strategy, your business will likely benefit from outside, independent information security subject matter expertise. For most small to medium-sized businesses, having a dedicated in-house security chief is not feasible.

According to Lam, "patching your systems is the #1 thing you can do to protect yourself." And without a vulnerability scanner, a company cannot address the issues in their system because they do not have the tools to discover those issues in the first place.

Another critical aspect of maintaining your information security is knowing the right questions to ask of your vendors. According to Majzoub, some key areas to cover include viewpoints on backup procedures, how and where data is stored, and the importance of cybersecurity training. In a recent webinar for Trusted Advisor, Lam summarized four critical questions as:

- Do you have policies and standards?
- Is someone qualified in charge?
- Have you had an outside audit done on your Information Security practices?
- Are you following community Secure Development Standards in developing your software?

"There is simply too much at stake for companies to place blind trust in technology partnerships." – Muhi Majzoub, Chief Product Officer, OpenText

Three Initial Steps to Secure Your Information

There are three basic steps to take towards locking down your information security:

1. Set policies and standards
2. Place someone in charge
3. Meet once a month

These steps may seem to be an oversimplification of an overly complicated process. But that is part of the point. To tackle the mammoth undertaking of securing your information, take it one step at a time and commit to methodically solving your internal issues.

With the help of information security experts, policies and standards are simple to put in place. Once this step is done, you will have established key performance indicators that can be tracked over time.

Putting someone in charge is a critical step because it establishes accountability. And meeting once a month ensures that information security stays top of mind and can continue to gain momentum as your team gets trained.

How Will You Respond to Clients?

Following an updated set of policies and standards is not foolproof. It is still possible to get hacked. But if that happens, you can say, look, despite doing all of these right, our systems still got taken over. While this changes nothing about the attack on your data, you may retain key clients that you otherwise would have lost.

In an interview with Trusted Advisor, CISO David Lam elaborated on a falsehood that pervades throughout the business world. "The myth is that management

thinks this is an IT problem. And that is a dangerous myth. Because first, IT does not have a risk perspective. IT has the perspective of, 'I've got to get this to work.' IT has the wrong view and the wrong training to assess risk. Secondly, who is the last person you want to ask whether they're doing a great job? Well, that person."

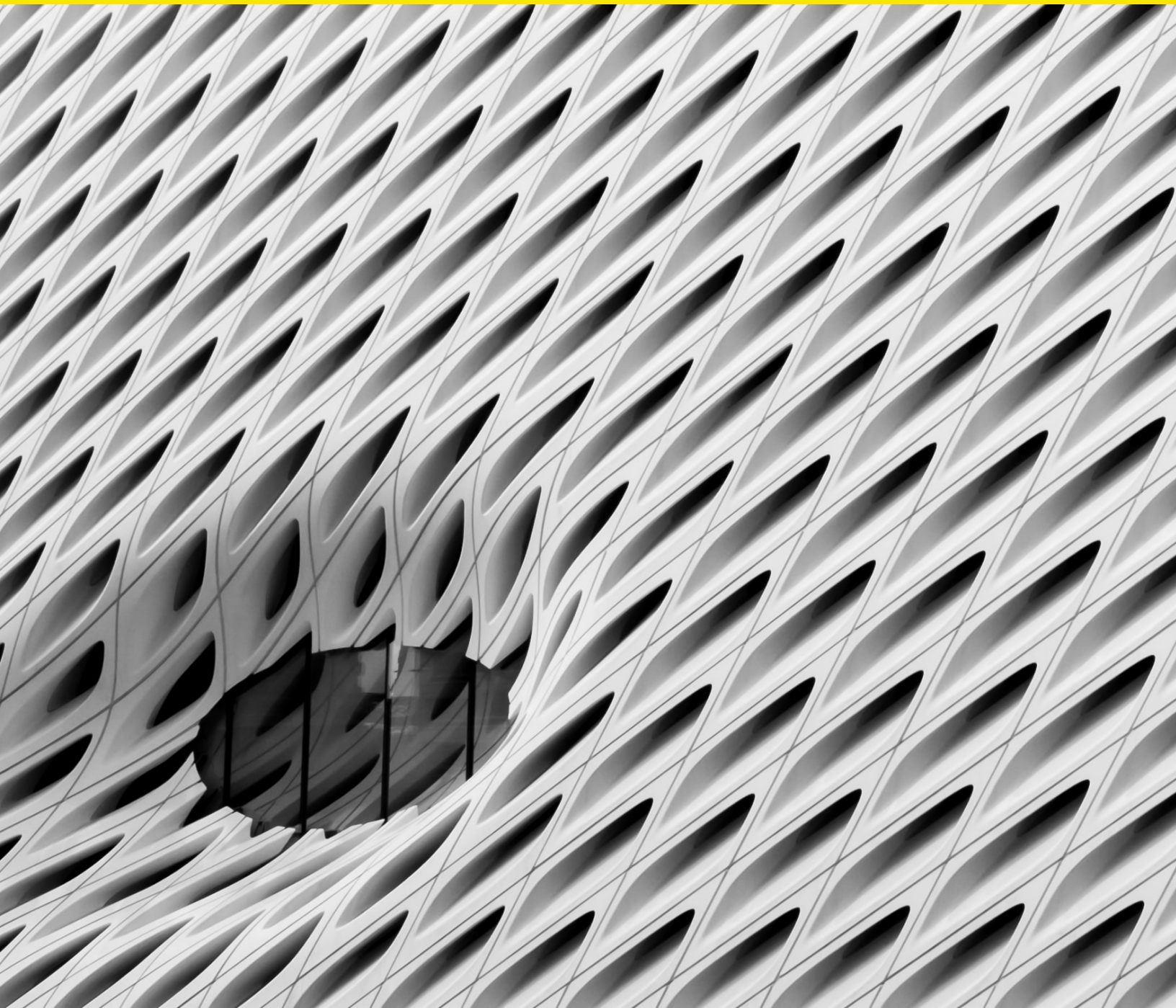
"So, here's what goes on. Management goes to IT and says, 'Hey IT, how are we doing?' And IT comes back and says, 'we're rocking it, we're awesome.'

We have never, ever, gone into a firm and come out going, 'you guys are 100%.'"

You Cannot Carry Out an Information Security Strategy Alone

While information security feels like it should be an IT problem, the reality is that InfoSec is not IT's job. Technology has accelerated so rapidly over the past decade; it has left many businesses trying to catch their breath to stay prepared and responsibly protect client data.

The companies that will not only survive but will thrive in this era of modern technology will be the ones that methodically secure their business from the inside out, one layer at a time. And with an information security management program in place, responsibly securing your data is readily achievable.



Trusted Advisor

Trusted Advisor is a dedicated resource for advisors of high net worth clients in the Entertainment space. We reach a tight-knit & exclusive group of about 10,000 business managers, music managers, and other entertainment advisors with A-list celeb clients, show-runners, athletes, musicians, influencers, writers, creators, and producers.

We regularly publish detailed reports on issues, technology, and news that affect advisors with entertainment clients. Please see more at: trustedadvisor.la

To learn more about Trusted Advisor you can reach us at: news@trustedadvisor.la

And a thank you to our Partners:

Miller Kaplan

Listen, then advise. That's what makes Miller Kaplan one of the top 100 certified public accounting firms in the United States. Established in 1941, Miller Kaplan has been providing audit, tax, business management, licensing and royalties, industry metrics, information security, and consulting services, to individuals, businesses, and tax-exempt organizations for more than 75 years.

See more here: https://www.millerkaplan.com/