20 Best Practice Recommendations for Improved Cyber Security Protection

A Report by P20

September 2021

Foreword

The COVID-19 pandemic has been a gift to cyber criminals, scammers and other bad actors. These organizations thrive on disruption, confusion and uncertainty. The overnight move to work from home and the closing down of life as we knew it presented a wealth of opportunities to those with nefarious intentions. As the world moved online en masse, the state sponsored and professional criminal gangs exploited the weaknesses of our security apparatus and the fears of individuals.

Since March 2020, cyber crime has rocketed. According to BAE Systems in a report on financial services, 74% of banks experienced a rise in cyber crime in the first year of the pandemic. Detected criminal activity rose by 29% while security budgets were cut by an average of 26%. Approximately 3 out of 4 financial institutions surveyed worry about the historic rise in criminal activity and what will happen going forward. And a similar number of consumers have personally noticed the increase and more than half believe responsibility for protection lies with financial institutions.

Jerome Powell, Chairman of the Federal Reserve, said in April 2021 that he worried more about the financial system being brought down by a cyber attack rather than a 2008-style crisis. This concurs with the view of the 23% of consumers who worry more about cyber rather than physical crime.

> Cyber security is no longer just a technical issue.
> As FBI Director Christopher Wray said in June 2021:
>
> "There's a shared responsibility – not just across government agencies but across the private sector and even the average American."

This report contains 20 Best Practice Actions for improved cyber security protection from cyber security professionals but the report's primary audience is the non-cyber professional. Everyone has a part to play in protecting their organization and its reputation by understanding where risks lie, questions that should be asked and simple actions that can be taken to enhance security.

I would like to thank all those who were interviewed for this report. They represent leading financial institutions, cyber security professionals and government officials.

I hope you find this report interesting, challenging and useful.

Duncan Sandys
CEO, P20

Recommendations

Network Security

- Assess, scan & identify everything that's connected to your network.
- Keep software and devices updated and back up all data to a separate location.
- Identify critical assets and assess how they are being protected.
- Ensure work from home users have updated routers with no default passwords.
- Develop an understanding of the risks associated with your supply chain network.
- Determine your ability to detect attacks and respond to them.

Data Handling

- Identify what data is important to protect, tag it and develop a protection plan.
- Develop procedures for handling data.
- Understand your digital identity, what that means to bad actors and how this information might be used by them.

Employee Awareness

- Create an organizational culture where everyone understands that cyber security is a business risk and cyber defense is everyone's responsibility.
- Ensure cyber security is a C-suite and Board priority and appropriate investment is made.
- Develop an annual cyber security training and education program (including practical exercises) to ensure the entire organization including supply chain understands the risk.
- Build a multi-disciplinary crisis management team across business and technical departments and encourage relationship building.
- Develop crisis management and business resiliency/disaster recovery plans, processes and procedures and test them in tabletop exercises.
- Ensure all employees understand that any email, link or attachment could be an attack source.

Things To Do Before A Cyber Attack Occurs

- Engage a law firm and forensic incident response firm and place contact names and numbers in your mobile phone.
- Develop an incident response plan documenting processes, print out hard copies and test the plan through regular tabletop exercises, including with external counsel, a forensic incident response firm and law enforcement, making updates as necessary.

Things To Do Immediately After A Suspected Cyber Attack

- After confirming that it really is a cyber attack, assess the initial severity of the attack, including the scope, apparent impact to the organization's IT infrastructure, sensitive data potentially affected and unknown variables.
- Convene your incident response team and implement the processes documented in the incident response plan. Consider internal escalation protocols, including C-suite and Board notifications, and alert legal counsel, your forensic response firm, law enforcement and report the incident as required to regulators, other governmental authorities and impacted individuals.
- Prepare communications to various stakeholders, including employees, customers, regulators, business partners, insurers, media and law enforcement.

Michael Papay, EVP, Technology Risk & Information Security American Express

If you could wave a magic wand and get a leader to do one thing relating to cyber security, what would it be?

One thing leaders often fail to do in cyber security is to really think about what it is we're trying to protect. Everybody immediately wants to jump into the details and figure out the technology, but very few people stop to think about what's important to the company, what's important to my organization, and what do I want to protect? After answering those questions, then you can think about how you want to protect.

In relation to network security, where do the greatest vulnerabilities lie and what is the best approach to tackle them?

The greatest vulnerabilities in the payments network are those hidden third-parties or fourth-party suppliers that nobody has identified as a risk. A lot of the big companies involved in payments networks understand the challenges -- they understand information security; they know how to approach these problems and how to tackle them. It's the smaller companies that are providing some critical service that we haven't fully solved for yet. You need to make sure those firms are doing a good job at information security, that they have the resources that they need, and that if they go down, the entire payments network stays resilient and doesn't go down.

What principles should organizations employ in relation to data handling?

This goes back to what I shared earlier about identifying what's important to the company and knowing what to protect. If you're handling a bunch of data, you've always got to consider: is this something that is important for me to tag and understand? I can't protect everything. I can't protect every single piece of information in the company, so I protect what's important. I identify what's important, tag it as important, then I can start putting my systems and other protection systems in place so that I know, "I don't want that to go out the door".

For a non-cyber professional without any cyber security training, what key things should they have an awareness for?

Every person should understand that cyber defense is their responsibility. It's every employee's job to protect the company, to protect the network, to protect the data – and they have to understand that spearfishing is still the number one threat vector out there. They have to watch each email that comes in and think critically, "Could this be an attack? This might be something bad. Maybe I should ask somebody or I shouldn't click on that link" – because that's still the number one vector for getting in. Each employee has to understand that and understand the repercussions of not playing their part in cyber defense.

Immediately following a cyber attack, what are the key areas leaders should focus on in those critical first hours?

It's a common refrain among chief information security officers: the first report from the field is often wrong. You might look at something, and think, "This is bad, we've been attacked." Ok, maybe that's what happened, but take your time. Work through the details, relax, and do your job. Because what often looks like a cyber attack really isn't. You have to train yourself to not just be reactive all the time. Take a moment to consider: this could be a network failure, this could be a third-party being

Michael Papay, EVP, Technology Risk & Information Security
American Express

"The greatest vulnerabilities in the payments network are those hidden third-parties or fourth-party suppliers that nobody has identified as a risk."

Watch Michael's video interview here.

down, this could be a cloud outage -- this could be a lot of things.

If it is a cyber attack, initiate your incident response plan. Every organization should have a plan written down and printed out should a worst-case scenario arise. And they must understand how to execute it. That means drilling and practicing the plan until it becomes instinctive. American Express does that across the board with our executives and with every critical element of the company.

When you confirm something is a cyber attack, a key part of the incident response plan is communication. You have to communicate to the executives to let them know what's going on. And you have to communicate to the technical teams so they understand, "This is my job and I need to execute immediately." And the only way to get that right each time is through practice.

Do you believe that you can ever reach a point when one can say "I have done everything and now I am safe"?

I'm pretty sure you haven't interviewed anybody who said, "Oh yeah, we'll get there." You know, I feel good. Right now, right at this very moment. Tomorrow might be totally different, this afternoon might be totally different, but it's a continual process. And that's what I love about the cyber business -- it's a continual process, it's always fresh, it's always changing, and you can never just sit back, relax and think, "Alright, I'm good. I don't need to work on anything, I don't need to keep current, I don't need to share any information or talk to anybody." You take some comfort knowing you've got a plan that you've rehearsed and you've got a great technical team doing great work. That's the only thing that makes you feel good, the only thing that lets you sleep at night.

Paul Collins, Regional Information Security Officer, Europe, Elavon

If you could wave a magic wand and get a leader to do one thing relating to cyber security, what would it be?

One of the challenges we have is security is typically seen as a technology issue. It's not. And what we really need to see is, from the top down, a tone change where it's accepted that security is the responsibility of everyone. I've heard references in the past that our users are our weakest links. They may be but they're also our strongest tools and our most effective resources. We need to develop a culture where people, when they hear security, don't just look to me but look around at each other and start to accept that they have a role to play.

In financial services, regulators are issuing enforcements and fines where senior management have not developed "a culture of appropriate risk management". Living by the letter of the regulation is no longer sufficient.

In relation to network security, where do the greatest vulnerabilities lie and what is the best approach to tackle them?

Firstly, legacy devices – there's always something on the network that people have forgotten about which no longer has support. Secondly, from a third party breach in a supply chain to which there is a direct connection. And we're also seeing the risk of our home network users. How does an organization know all of its employees' home routers are updated and don't have default passwords set.

In some cases, we're not necessarily looking at a vulnerability but rather a misconfiguration. And then there is what we used to call fat finger syndrome when someone just pressed the wrong button. Finally, there are open connections that were opened at one point to allow a particular user to come in the network that may still be open and vulnerable to attack if somebody can find them.

In short, you need to have the tools to assess, scan and identify everything that's connected to the network and then have the ability to mitigate.

What principles should organizations employ in relation to data handling?

In one word, it's proportionality. It comes back to knowing where your information assets are and what controls you have around them. You don't need to have the same level of control for all of your data but you need to understand where your crown jewels sit and make sure that you've got appropriate security around them.

And when I say appropriate security, I'm not just talking about technology. A lot of the most effective security controls are procedures. They are actual actions that people can take in terms of how they handle data and the level of care they take with a sensitive or valuable asset. needs special care.

What do you consider to be the single biggest cyber-related mistake people make and how can this be addressed?

It's using the same password on multiple systems. So, you have your same password for your email, internet banking, Facebook. And the problem is that at some point, one of those environments is going to be breached and your data is now exposed. And the same guys who get that data are going to try Facebook, Amazon, Google, your bank accounts, to see if they can get in.

There's a website called **Have I been pwned?** You can enter an email address or a phone number and it will tell you if that information has been exposed and whether you need to take any steps to address that.

Paul Collins, Regional Information Security Officer, Europe, Elavon

"The simplest advice I can offer is to treat your password like your toothbrush: don't let anyone else use it and change it regularly."

Watch Paul's video interview here.

In terms of mitigation, there is a simple approach. You can install a password manager app to store all of your passwords.

But the simplest advice I can offer is to treat your password like your toothbrush: don't let anyone else use it and change it regularly.

Immediately following a cyber attack, what are the key areas leaders should focus on in those critical first hours?

The most effective thing I have seen is to get a multi-disciplinary team together as quickly as possible. And I'm not just talking security people here. One of the key resources you need is a communications person who can package your message. And what we're seeing is that once regulators see news of a breach, they're going to start asking questions. You have to start capturing information as quickly as possible and preparing the answers to questions.

There was always this fear in the past that if you were breached, your reputation was shot. I think that's moved on. There's an acceptance that some threat actors are nation-state bonded and incredibly well-resourced. If they choose to attack you, they're probably going to be successful. So, it's not so much about stopping them getting in but what you do when you are attacked. The manner of your response will dictate far more about your reputation than the actual breach itself.

What you will often see is that some ex-law enforcement security officers rely on their own personal networks in order to lead how they respond. And I think the regulators are saying that's not good enough any more. We need to have something more structured, more formal and more integrated.

Do you believe that you can ever reach a point when one can say "I have done everything and now I am safe"?

No. If you look at the amount of technology, every new piece is a new source of vulnerability or weakness.

With all this technology, you've got sources of information, systems that aren't ever going to be 100% patched and 100% secure, you're always going to have some source of vulnerability. And it's only getting more complicated. And in some cases, they will extort or coerce an employee into giving up their password and with that, it doesn't matter what security controls you have in place.

Peter Marta, Partner, Cybersecurity & Privacy Practice, Hogan Lovells

Is cyber security generally and are cyber attacks in particular something everyone should be concerned about?

Absolutely. All you need to do is glance at the papers these days. Cyber attacks are constantly in the news. One of the mistakes that companies make is thinking that they're not a potential victim. The reality is that every company in every industry really is a potential victim of a cyber security attack. There's the famous quote that you often hear from a former director of the FBI in the US that there are two types of companies: those that have been attacked and those that will be attacked.

In relation to network security, where do the greatest vulnerabilities lie and what is the best approach to tackle them?

In terms of network security, having basic cyber security hygiene is important, things like multi-factor authentication. We see in a lot of the breaches today that phishing is often a common vector of attack and in addition to basic cyber hygiene, employee awareness is really important and can't be over emphasized. Employees are often the weakest link. In fact, I think they're always the weakest link and reminding employees about the importance of proper cyber security best practices is important. Requiring at least annual cyber security training and doing things like phishing exercises is certainly best practice these days.

With regard to data, how do you increase the understanding that what people are handling is a valuable commodity of great interest to bad actors?

People in organizations should understand that regardless of what industry you're in, threat actors are out there. They're interested in trade secrets but they're also interested in making money. And one of the mistakes companies make is thinking, they're not in the right industry, they're not the biggest player in their industry. That's misguided in many cases. These are criminals and they don't care if it's a global financial institution or a mom and pop widget maker – they just want to get paid. And in fact, it's more likely in some cases that a threat actor will go after the low-hanging fruit because why would you attack a global financial institution that spends hundreds of millions of dollars on cyber security when you can attack a mom and pop widget maker that spends a fraction of that.

How do you address and reverse the "it won't happen to me" trend?

It goes back to the idea that organizations should understand that anyone is a potential victim, and that really is a key takeaway. If you use a computer, you are a potential victim of a cyber security attack. Threat actors, in the case of ransomware, just want to get paid. They don't care who the victim is. In some cases when they initially hit a victim, they don't even know who they're hitting. They want to get paid. And so organizations need to understand that anyone in any industry of any size in any geographical location is a potential victim of a cyber security attack. And so you really have to have the mindset of it's not if, but when.

In the event of an attack or a breach, there is often confusion as to who to call. Who would you recommend be the first external person to be informed?

Best practice today is to contact outside counsel. They will often then be the one to engage a third-party forensic firm, so that everything after that, the investigation, any type of report that is prepared

Peter Marta, Partner, Cybersecurity & Privacy Practice, Hogan Lovells

"Organizations should understand that anyone is a potential victim. If you use a computer, you are a potential victim of a cyber security attack."

Watch Peter's video interview here.

will be protected by attorney-client privilege. And it is important to understand that ahead of time and put in place a relationship with a law firm and a third-party forensic incident response firm, so that you know who to call and you know how to call them. I ask my clients to put my personal cell phone number in their cell phone so that inevitably on Friday afternoon or Saturday evening when an attack is detected, they know how to contact me.

But I've seen some situations where there's an individual in the security department who is former law enforcement, and when something happens, before coordinating with the legal department and outside counsel, they pick up the phone and call their friends at the FBI or overseas equivalent. And that can be helpful but it's also problematic because now you have outreach to law enforcement that is uncoordinated. You don't necessarily have the proper message in place. So, I recommend engaging with the legal department, outside counsel, talking about it ahead of time and having a strategy for reaching out to law enforcement. And I am a particular proponent of reaching out to law enforcement for a variety of reasons and in almost every situation that I've dealt with, I have helped facilitate that introduction.

Do you believe that you can ever reach a point when one can say "I have done everything and now I am safe"?

No. Just like many issues in a company, cyber security should be viewed as investment. And as threat actors become more sophisticated, as threat vectors evolve, companies and organizations need to evolve their cyber security best practices and programs. You can be right 364 days out of the year. Bad guys only have to be right once. And so I don't believe that you can ever get to the point where you're entirely secure. That goes for governments as well as private sector organizations. So again, my view is to view cyber security as an investment, not just a cost.

JF Legault, MD, Global Head of Cyber Security Operations, J.P. Morgan Chase

What do you believe to be the most misunderstood concept about cyber security?

I wouldn't go down the road of misunderstood concept but I would focus on the operational resiliency aspect of cyber security. Meaning the role that cyber security plays in ensuring the availability of services that are provided to consumers. That ranges from security monitoring roles, detecting threats and mitigating them all the way to discussing technology and business resiliency and running tabletop exercises. So historically, there's been a lot of emphasis put on the C in CIA, on the confidentiality aspect but there's been more and more work that's being done on the integrity and availability aspects. So, when you think about resiliency, it's really about making sure that the service continues to be provided to the end consumer.

What do you think network security means to a non-cyber professional and what do you regard as essential knowledge everyone should have?

Historically, if you look at the evolution of security, when I started doing this, we called it Network Security, and then it evolved into Cyber Security, Information Security. So, there's been a lot of terms that have been used. And I think what's important to understand is that when we talk about network security, it kind of evokes a history of a strong perimeter. But what we're dealing with today is a dissolving perimeter for organizations. There's a reliance on third party software as a service or talking about moving to the cloud. So, it's really for an organization to rethink what their perimeter means to them and how do they adapt their defenses. If we're talking to the overall, what it evokes for me and what it means is really looking at how we're securing our most valuable assets in a context where we don't have a strong brick and mortar perimeter any more.

With regard to data, how do you increase the understanding that what people are handling is a valuable commodity of great interest to bad actors?

I think it's awareness – can't say this enough. Every time I have meetings with organizations, it's about driving awareness on how information can be used by an adversary and what it means to them. Some people often forget how adversaries can use information and at times there's a focus that's placed on credit card data, personally identifiable information but there's elements of information that can help an adversary target individuals that can help them refine their techniques, tactics, and procedures (TTPs) against an organization.

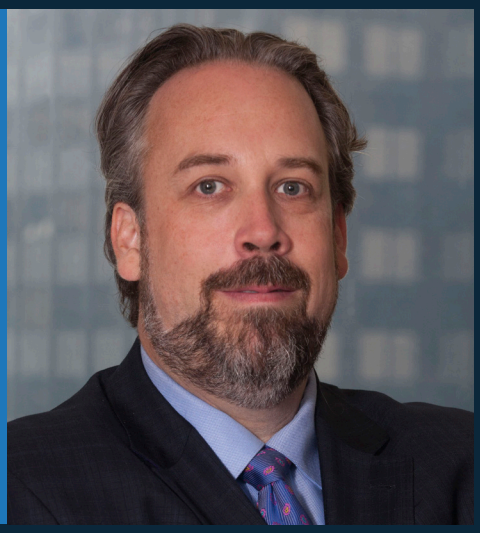
For a non-cyber professional without any cyber security training, what key things should they have an awareness for?

When you consider the most critical aspects, it's really around crisis management. And it's having relationships. Too often you'll see the business side and the technology side meeting for the first time during an incident. And you don't want that. The key here is how do you build an organization that is resilient, and how do you build strong crisis management functions whereby the technology teams and the business teams play a role together in mitigating risk for the organization? One of the ways to do that is through tabletops. It's simulating scenarios of an attack, of ransomware, of a variety of different threats to the organization and bringing together all the parties that would be involved in dealing with that scenario. And that really includes business, tech, legal, media relations, HR, corporate security, all of the key players are around that table and have a common understanding of each other's roles, but also their challenges in the case of a crisis.

JF Legault, MD, Global Head of Cyber Security Operations, J.P. Morgan Chase

"You can have the strongest controls in the world, the best cyber security program but one thing that organizations continuously need to work on is improving their crisis management processes."

Watch JF's video interview here.



Planning is key, planning for an incident is key. You can have the strongest controls in the world, the best cyber security program but that one remaining thing that organizations continuously need to work on is improving their crisis management processes. If you look at a lot of the crisis management processes in organizations, they were designed for people to sit in the war room So everybody would be brought into a war room, give regular updates and then we got a global pandemic which prevented people from being in a war room to run a crisis. So, think through all of the potential scenarios, even using very far-fetched scenarios, just to trigger a thought process as it forces the organization to adapt, evolve, and improve its processes.

At the moment someone realizes a cyber attack has occurred, what immediate actions would you recommend be taken?

It depends on the nature of the attack. And it goes back to having a process that's documented, having a guiding principle. So the first thing is very much reaching either physically, logically, or virtually to that incident management playbook that guides who should be involved. That means having put some forward thought into, "what do I do if this happens?" And the critical aspect is keeping people informed: information dissemination, communication is key during a crisis. As a technologist, my job would be to keep the business informed of the threat landscape, the remediation, the mitigation that's ongoing but it's also for the executive team to communicate to me what their priorities are – but if we've never tested that out, we don't know what each other's roles are. So, there's a lot that needs to happen before the crisis hits.

Do you believe that you can ever reach a point when one can say "I have done everything and now I am safe"?

You'll never reach that point. Anybody who says that they've reached that point is not keeping an eye on the threat landscape. The threat landscape changes on a regular basis. Adversaries evolve, controls evolve. There's an element of having a threat informed cyber security program so that you can actually track where adversaries are going, where threats are increasing, and adapt your controls, adapt your processes to dealing with those specific threats.

Paul Maddinson, Director for National Resilience & Strategy, UK National Cyber Security Centre (NCSC)

If you could wave a magic wand and get a leader to do one thing relating to cyber security, what would it be?

There isn't one single silver bullet that can solve all of your cyber security issues. The one thing we would like leaders to do is take a holistic approach to cyber security. And what I mean by that is don't treat it as a small technical issue that your technical department can fix. But look at it as a business risk issue, understand how cyber threats might pose a business risk and then take the normal steps you would to both mitigate that risk and to prepare for incidents. When things go wrong – and with cyber security there will be incidents – you need to be prepared so you know how to respond. On our website **ncsc.gov.uk**, we've got **10 Steps to Cyber Security** that will help you create that holistic approach.

How does a small organization with limited funds ensure their network is secure? What essential elements should they focus on?

We recognize that it's a difficult challenge for smaller organizations to get a grip on cyber security and the key things to get the basics right. We promote some advice for small organizations and there's a really good cyberaware.co.uk website where you can create an action plan. There are several things that we recommend for small organizations to get those basics right. One is about backing up data and making sure you're doing that properly. The second is using passwords appropriately. The third is keeping your devices updated and making sure that the software is patched. The fourth is putting some protections in place against malware and then trying to avoid phishing attacks through email and how your staff respond.

What types of actions can reduce the attractiveness to a criminal of attempting a data hack?

Criminals are largely opportunistic. They'll often target the victims that are the easiest.. And one of the ways they do this is by exploiting known vulnerabilities. When a vulnerability is discovered, criminals scan the internet to identify people who have that vulnerability and then exploit and attack them. That bit of advice I said earlier about updating your software and making sure you apply patches so that your software does not have known vulnerabilities is probably one of the best things that you can do. Secondly, be aware that if you've got a large internet profile and your ways of working are accessible then you're potentially more targetable by criminals. So be very, very aware of your digital identity and understand how that might make you more attractive to criminals.

For a non-cyber professional without any cyber security training, what key things should they have an awareness for?

This goes back to what I said at the beginning, which is the first thing is to understand cyber security as part of a business risk. For that, you need to understand the key elements of your business or organization that might be threatened in a cyber attack. Understand that it's a business risk and then make sure it's been discussed in those terms. We have a board toolkit on our website which helps boards to get to grips with this as a business risk issue, to follow through by identifying what it is that's and to take the steps to implement the necessary mitigations.

Paul Maddinson, Director for National Resilience & Strategy, UK National Cyber Security Centre (NCSC)

"For an organization that gets a better grip on cyber security risks and starts managing them in a professional way, it can be a differentiator in the future."

Watch Paul's video interview here.

In the event of an attack or a breach, there is often confusion as to who to call. Who would you recommend be the first external person to be informed?

In the UK, the first person to call is Action Fraud or in Scotland, Police Scotland, because cyber attacks are a crime and it's important that they are reported to law enforcement. They will look at what assistance they can give. After that, the second place to go is for the professional assistance you need in order to respond. If it is a significant cyber incident in the UK, the NCSC can either help you directly or point you to qualified and accredited companies. It's quite important to get that professional expertise as well as report it as a crime. As the incident progresses and people understand what might have been affected, it's important to consider any legal or regulatory reporting obligations you have. For example, with a data breach in the UK, there's an obligation to report it to the Information Commissioner's Office if it affects personal data.

Do you believe that you can ever reach a point when one can say "I have done everything and now I am safe"?

Unfortunately not. That sounds a bit negative but the reason is that cyber threats continue to evolve rapidly and the technology we use and rely on is also changing very, very rapidly. So unfortunately, it's not possible to say you've done everything and you'll be safe. Like many risk areas, this is about risk mitigation. And so it's an ongoing activity.

But on the more positive side, for an organization that gets a better grip on cyber security risks and starts managing them in a professional way, in a way that businesses run a lot of other sorts of issues that they cope with, it can and will be a differentiator for organizations in the future. Those that are not vulnerable to cyber attacks, those that have resilience and can continue to provide their services and their goods will do better in the world. And those that can exploit technology securely will benefit. So unfortunately, I don't think we can ever say that you're secure but ongoing management of cyber risk in a professional way is a good thing for an organization to achieve.

Linda Lacewell, Former Superintendent of Financial Services, New York State Department of Financial Services

So is cyber security generally, and are cyber attacks, something everyone should be concerned about?

Yes, absolutely. Cyber security is a critical issue of our day. And it's critically important to everybody. If you're an individual, a consumer or a small business and your accounts are hacked or taken over, and your privacy is invaded, you've got to worry about rebuilding your credit. That could be downstream from a much larger cyber security attack and so cyber security is really critically, critically important.

And it is so important because the next financial crisis could be triggered by a cyber attack, given how large our key financial institutions are, how interconnected they are, and how major payment processors are connected between them. The Chair of the Fed is more worried about a cyber attack than he is about the kind of factors that triggered the last financial crisis in 2008. So everybody should be worried about it. But I think it's important not to feel overwhelmed. There are things that everybody can do, should do, and must do to protect themselves, their counterparties and the security, in fact, of the nation. It's not too extreme to say.

How do you address and reverse the 'it won't happen to me' trend?

Denial is not a life strategy. But the first step to any problem is recognizing the problem. Now, it's important not to feel overwhelmed. I think of it this way. If you live in a high crime neighborhood, you don't throw up your hands and say, "well, what's the point of locking my door?" Lock the front door. Get an alarm system. Be vigilant. Work with your neighbors. There are a lot of things that you can do to make yourself not the low hanging fruit. For financial institutions that have such an impact on people's lives and the economy, we put out a number of principles that they should abide by. And we also require them to report to us any material intrusions, especially if it may affect consumers.

But it's got to be a priority. You got to make the investment. I know it costs money but you are protecting the company. You're protecting your own asset, protecting your employees, you're protecting consumer information, your intellectual property. So it's got to be a priority for the executive suite. It's got to be a priority for the board of directors. The tone has to be set at the top. And we need continual vigilance and training of employees.

Why is the risk from cyber threats continuing to grow?

We live in an increasingly digital society. And that's very exciting. But the more digital we become, the more digitized our information becomes. The more digital our companies become, the more the security of those systems is about cyber security. And that maximizes the ability for intrusions, making cyber security the leading counter-terrorism, financial and financial security issue.

Cyber attacks are a tool of those who want to undermine US interests and of cyber criminals who would like to make money. One of the really pressing issues is a ransomware attack. Do you pay the ransom? And it may sound like a pretty simple question. Of course, I care about what's at risk here. I'm going to pay the ransom. Except, given the sophistication of these criminal gangs, state actors and terrorists, they will plough that money back into their cyber attacking enterprise. And this will go on.

What we really need are individuals and businesses, especially large businesses and large financial institutions, to do everything they can to improve their own security. But we need the federal government to be highly focused as a matter of safety and soundness of industry and our financial

Linda Lacewell, Former Superintendent of Financial Services, New York State Department of Financial Services

"Cyber security is a critical issue of our day. And it's critically important to everybody. It's got to be a priority for the executive suite. It's got to be a priority for the board of directors. The tone has to be set at the top."

Watch Linda's video interview here.

system. Because if the next serious cyber attack on a financial institution triggers a liquidity crisis, what matters are all of the consequences of that.

If you wake up one day and you notice some ATMs are frozen or bank accounts no longer register balances, is there going to be a run on the banks? How are banks going to know, if the payment processor can't track the payments any more, what the funds flow is? Everything happens on an automated basis and gets settled. The system moves very fast. And these kinds of attacks could be devastating.

One of the things to bear in mind about these crises is you don't actually know how it's going to unfold. But the possibilities are a bit terrifying. And that's why last month the White House released a letter urging all American businesses to pay attention and to adopt key measures to maximize cyber security, such as multi-factor authentication. That's like the ABCs at this point: encryption, incident response, planning, vulnerability management, elevating cyber security – a job which is really never done.

Do you believe that you can ever reach a point where you can say, "I've done everything and now I'm safe"?

I wish that were the case. I really do. The problem is the attacks are becoming more sophisticated. And I think that the SolarWinds attack was shocking to a lot of people in terms of the level of sophistication and the methods and means that they were using. We can't let that stop us. If you're starting at zero, start working. It's better to get up to 30 and 50 and 70 and 80% secure and just keep going, rather than ignoring it. It's like any problems we have in life, get started and keep going.

Phishing is a major gateway into cyber attacks. So the training of your individual employees and what they click on is critically important. How do you make sure that they're not inadvertently letting somebody into the system, unlocking the door, by clicking on the wrong link? Every business, every agency, every financial institution needs to do that.

And I look forward to an all of government approach to cyber security because we are such an interconnected government, society and nation that we've got to strengthen the system everywhere because we're only as strong as our weakest link. And if somebody gets in through that weakest link, it can affect everybody else.

Jason Crabtree, Founder & CEO, Qomplx

What do you believe to be the most misunderstood concept about cyber security?

I think cyber security currently suffers from learned helplessness. We have to create a spirit of capability and actual investment in defensive mindsets from non-technical executive leaders so that we're capable of rapidly detecting and responding to events. We must communicate honestly with our constituents, whether they're consumers, shareholders or regulators. I think the more that we get out of this "we're not responsible for our outcomes, we couldn't possibly defend ourselves against nation states" etc, the faster we're going to start to have really healthy discussions about what we need to do to be both collectively successful and individually successful -- so that cyber security is no longer just the scourge of ransomware and other events shutting down our businesses.

If you could wave a magic wand and get a leader to do one thing relating to cyber security, what would it be?

The most important thing people need to do is get visibility into their own networks, including how they look to prospective attackers. Having a culture where people are going to help establish that visibility and raise issues that are being faced so that we can put in place different types of defenses to disrupt and interdict these kinds of attacks, quickly and forcibly matters. A lot of organizations are still not having sufficiently candid discussions internally or they have too much of a maturity model and compliance-focused mindset where they're ticking boxes and not asking, "what do we look like from the perspective of someone who would like to ransom our organization or go after our customer data. We've got to have this offensive mentality based on realistic threat models and scenarios to be effective on the defensive side.

How does a small organization with limited funds ensure their network is secure? What essential elements should they focus on?

This requires a mix of people, process, technology and data. And a lot of organizations don't necessarily want to do their homework or start with the necessary basics. The basics are: do I collect the information I need to see these kinds of attacks at all? Do I move that important information to a centralized location? Do I store it? Can I search it? Do I keep it for long enough that I'm going to be able to go back and look for a compromise? And then do I have the ability to build detections? Can I scale those? Can I use this information to actually look for adversaries on an active basis, both outside of my network, so looking at myself from the outside as well as inside out? You have to build this gradually based on ground truth.

And the degree of completeness might vary if you're very large with the ability to resource this in a formidable way or if you're very small; but, the fundamentals are not any different. You've got to have visibility in the right locations so you are able to detect and respond. You have to have the trained staff to do it. If you aren't doing that, you aren't doing security, you're doing theater.

What types of actions can reduce the attractiveness to a criminal attempting a data hack?

First, we're encouraged to see increased international cooperation and action taken by law enforcement that identify and prosecute criminal networks and individual participants. But that won't solve it alone. When it comes to cyber security, you don't want to look like an attractive target. A lot of the organizations being ransomed have stuff that's not supposed to be visible on the Internet. Many a lot of historically exposed password information from or poor identity management. Most have inadequate internal detections or visibility. So after an external foothold is gained or after a successful phishing or spear-phishing attack, which can be very convincing, there are really no impediments or resistance once you get inside the network.

A lot of these networks look like a raw egg. They have this thin shell on the outside but once you get inside, it's just goo. You can go wherever you want. We've got to make it more difficult for people to move laterally and that's why there is this focus on visibility, detection, response and in the case of ransomware, how to quickly restore from back-ups. The same organizations that are often getting targeted because they have weak external security postures are often the same organizations that either don't have back-ups or have never practiced using them. That's part why you see a lot of companies faced with a very difficult decision to pay a ransom because they may not have the maturity to restore from backups at all. We've got to get better at this as part of normal operations.

Jason Crabtree, Founder & CEO, Qomplx

"You've got to have visibility in the right locations so you are able to detect and respond. You have to have the trained staff to do it. If you aren't doing that, you aren't doing security, you're doing theater."

Watch Jason's video interview here.

How do you address and reverse the "it won't happen to me" trend?

The reality is a lot of the organizations that have this mentality are the same ones that look like a meal. That mentality is exactly what leads people to not look at their external posture like an adversary does. Criminal organizations or ransomware, and even sort of pseudo-state sponsored or tolerated actors all look for the same stuff. They look to get as much value for this little input as possible. So, if you have open, external vulnerabilities or if you look like an easy mark, you are really attractive to attack.

And if you're really attractive, you're going to get targeted above and beyond your peers. There's no magic in these ransomware attacks . They've largely been using the same techniques for more than a decade - they are just getting faster and easier. And a lot of the common gateways in are things that can be identified with a tremendous amount of vigilance and constant checking to find bad stuff faster than everyone else and fix it first.

For the most part, they're picking off the weak links at the back of the pack. And that reality means that you don't need to be Usain Bolt, you just need to outrun the slower campers in bear country and make sure that somebody is able to get a meal that doesn't look like you at the individual level.

Do you believe that you can ever reach a point when one can say "I have done everything and now I am safe"?

Cyber security is a continuous process. It's about constant engagement and vigilance to stay secure, not become secure. And why is that? Every day people are showing up to work and they're interacting with the world. They're exchanging data, they're opening Excel documents and PowerPoints that can have malicious macros. Your HR team or recruiting team is asking people to send you PDF documents because they're asking you to apply for jobs - some of those will be weaponized. Occasionally, they'll get through. People are going on the Internet. They're going to go and visit watering hole sites. They're going to get convincing phishing emails. You're going to make bad configuration changes to firewalls and VPN services. You're going to share information with your partners. As a result, this idea that you're not going to have a breach is foolhardy. The best thing you can do is acknowledge that this is going to happen. People are going to get inside your network.

Assume breach means make it difficult for someone to go undetected for long. Silent failures are terrifically poisonous, but rapid detection means that you can make really big events into small ones by making sure to catch them quickly. Make sure that attackers don't get administrative rights and make sure that they can't just go wherever they want in your network. And then inform the people that need to know about it.

That's going to be a healthy discussion for us to have as a community, as an industry. And if we're not having that kind of discussion, we're going to continue to see this. This is hard but an acceptably solvable thing. We should have a lot of hope about what we're doing. And if we're successful, attackers are going to choose new ways to attack our organizations and we're going to see the threat continue to evolve. That's a good thing. It means we are imposing cost. But that's going to require us to all embrace this idea that it's everyone's responsibility and acknowledge there's a lot of low-hanging fruit that we should all be out there focusing on. Focused effort is going to help raise the bar and help law enforcement and our instruments in national power and international partnerships to really put the pressure on the kinds of criminal organizations or bad behavior that we're seeing right now, but only if we improve defense at home.

Pankit Desai, Co-founder & CEO, Sequretek

What do you believe to be the most misunderstood concept about cyber security?

That cyber security is a people, process and technology problem. If you are a CEO, you may think you can outsource this problem to a technologist to solve it but if as a CEO you don't give attention to a business issue, most likely, it's not going to get sorted. A CISO works for a bank today and tomorrow he's going to work for a manufacturing company. There is no way the security construct in a bank will be the same as a manufacturing company. The only one who understands the context is the CEO and unless the context gets transferred to the technologist, you are in for big trouble.

What do you think network security means to a non-cyber professional and what do you regard as essential knowledge everyone should have?

Historically, the way organizations were structured was that you had physical premises with large data centers and most employees sitting in that physical office. Cyber security was a virtual security wall around the data center and the assumption was that if you had a strong enough wall with good enough security then you were protected against external attacks. So, network security primarily meant perimeter security. That's the past world.

In today's COVID and work from home world, more than at any time in the past, users have moved out of the premises and data centers have moved to the cloud. Even if you are a legacy company, you may be forced to move to the cloud because your existing infrastructure is not geared to support remote work environments both for the employees who use it as well as the IT teams who manage it. In today's context, there is a legacy realm of perimeter security but also a context of security where you need to decide if your data infrastructure and applications is going to be cloud based. And devices that are working from home and coming on public networks, how are they getting secured? So the perimeter is getting redefined as we speak.

In relation to network security, where do the greatest vulnerabilities lie and what is the best approach to tackle them?

There are four areas I can think of. The first is the traditional malware: viruses, malwares, spywares, ransomware and other types of wares. Primarily they'll go after devices like networks, laptops, desktops and servers. Second is called phishing, spear phishing, railing, different nomenclature for what essentially means is that you are targeted by exploiting your curiosity, arrogance or ignorance. They abuse publicly available information on an individual to get you to do something that you shouldn't do. Third is your outdated system. Unfortunately, as organizations grow, they forget that they are invested in scores of technology products which have not been updated and can be exploited. And a fourth area is that whatever perimeter systems that you've deployed, they are deployed to the optimum level.

For a non-cyber professional without any cyber security training, what key things should they have an awareness for?

For most companies or individuals, if you can get everyone to have this one simple understanding: that any email, link or attachment that comes from an unknown source is most likely going to be an attack and therefore to give it the right sense of caution before doing anything about it. That would be a single biggest thing that someone could do to reduce the ancillary risk that comes from people doing stuff that they ought not to do.

The second critical part is for you to understand where your assets are. So if you have a critical asset, you need to figure out where those critical

Pankit Desai, Co-founder & CEO, Sequretek

"Security is a journey. Environments continue to change, as do who you do business with, how you do business, your infrastructure and your capabilities."

Watch Pankit's video interview here.

assets are and what are the protections. If you were to be breached, what is the impact that that asset could have? The least you can do is to answer the question: where do your critical assets lie and how are they being protected?

Immediately following a cyber attack, what are the key areas leaders should focus on in those critical first hours?

If you have a fire in a building then the process is laid down. You have to identify where the fire is, contain it, inform the fire department Execute the evacuation plan. Everything is pre-planned. So, first and foremost is to have a plan – a plan for a plan. You have got to have a plan in case of an attack setting out what you have to do.

Assuming you have an attack, you first have to figure out a way to contain it so it can't spread. Unfortunately, attacks these days are not insular. They have a great chance of spreading and creating a lot of collateral damage within the organization. Second is to report it to the set of impacted parties. You have to go to law enforcement, you may have to report to a regulator, you have to report to the board, senior management, the whole hierarchy. Third is to investigate and remediate. You got to figure out where the problem is and how to remediate it. And the last part is to recover with short-term things to come out of it and recover in the long term to make sure that this event doesn't repeat itself in the future.

Do you believe that you can ever reach a point when one can say "I have done everything and now I am safe"?

Unfortunately, not. Security is a journey. You can't say it's done because environments continue to change, as do who you do business with, how you do business, your infrastructure and your capabilities. Just look at what happened with COVID. If in February 2020 you said, "I have done it all, I've invested, I'm completely secure", come March the world changed around you. The entire way you do business is completely different.

Sem Ponnambalam, Co-founder & CEO, xahive

Is cyber security generally and are cyber attacks in particular something everyone should be concerned about?

Cyber security is everyone's responsibility, especially now. This includes boards, executives, who should ensure that there are cybersecurity governance policies and procedures in place. This goes beyond just having state-of-the-art cyber technology. You need to ensure that the entire organization and value chain members are actually undergoing cyber security training and education, especially now that we're working in this hybrid model of working remotely and also potentially going back to the office.

Not using secure end point encryption is also a big issue. That has to be included, especially when you're communicating any sort of sensitive data that has personal identifiable information or personal health information, and it's vital that organizations actually undergo a third-party cyber security audit. But I do encourage all employees and value chain members to also undergo cyber security training because oftentimes, breaches don't happen internally. It could be due to your third-party vendors. So, especially now with everyone deploying digital transformation protocols with 5G and internet of things (IoT) being utilized along with artificial intelligence (AI), it's really important to make sure cyber security is everyone's responsibility.

What do you consider to be the single biggest cyber-related mistake people make and how can this be addressed?

Thinking that we're all safe and that cyber security issues should only be dealt with by your CIO or your chief information security officer or your IT team. You have to realize that cyber security is something that the entire organization needs to be aware of, concerned with, and should be taking every step possible to ensure that you undergo the required type of security training and education, and that you have good cyber security governance policies in place.

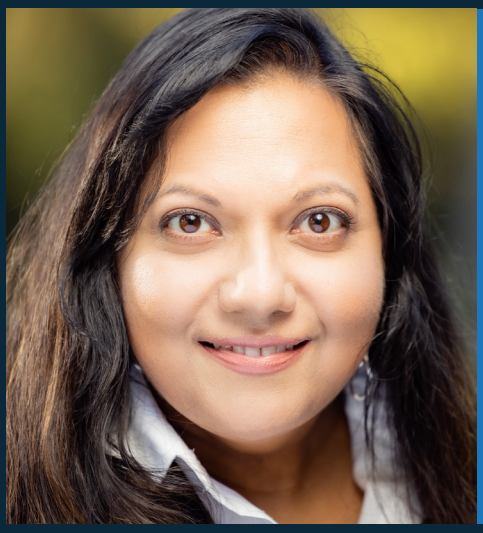
How do you address and reverse the "it won't happen to me" trend?

It's really important to understand that it is a matter of when you find out that you've been breached, not if you have been breached. So that mentality shift really has to take place. And it's also important to note that it takes on average over 228 days to identify whether your organization has actually undergone a breach, according to latest studies from IBM in 2020. So, you may not realize that you've been breached, but you have to really take into consideration that you have been breached and take all the steps that you need to ensure that you are constantly vigilant.

At the moment someone realizes a cyber attack has occurred, what immediate actions would you recommend be taken?

I would encourage someone to immediately report all the issues, open an incident report, document everything, and immediately convene your incident response team. This should include board members, senior management, technical reps, cyber reps, both within your organization and a third-party organization as well to come in to help you with the audit, your HR team, employee reps, people who are responsible for intellectual property (IP) within your organization, or privacy compliance rep, public relations rep, and of course, your legal reps and your cyber insurance representatives as well. So, it's really important to convene and then pretty much go through discussing the important findings with your key stakeholders and figure out steps to restore your operations.

Sem Ponnambalam, Co-founder & CEO, xahive



"Cyber security is something that the entire organization needs to be aware of, concerned with, and undergo training and education for, and you need to have good cyber security governance policies."

Watch Sem's video interview here.

In the event of an attack or a breach, there is often confusion as to who to call. Who would you recommend be the first external person to be informed?

I would recommend contacting a third-party cyber security company to come in to help figure out where things are: what are the gaps, what are the weaknesses, and how you can take steps to remediate? That would be your first step, and then they could work with your IT teams and isolate and suspend any compromised sections within your network, at least temporarily to figure out next steps. And then following that, I would recommend that once you've spoken to your internal teams, you notify law enforcement, and depending on your regulation or jurisdiction, you may need to follow through and ensure that you're complying with those reporting requirements as well.

Remember that law enforcement will not come in to fix the problem. They'll want to know what the issue is. So they'll take steps if there is any sort of business email compromise and money has been transferred. They'll recommend that you contact the financial institutions and then they'll begin the trace but if you don't know where the breach is or what the problem is, it'll be difficult for law enforcement to take the steps to do that because that's not their job. They're there to deal with the crime.

Do you believe that you can ever reach a point when one can say "I have done everything and now I am safe"?

Unfortunately, not. As cyber crimes become much more sophisticated, it's going to be a battle to continuously keep up with cyber criminals and state actors and identify ongoing vulnerabilities. With 5G becoming ubiquitous, there are a ton of legacy vulnerabilities that have been inherited from 4G technology, and 5G has over 200 times more cyber security access points or vulnerabilities, and with IoT devices rising on a daily basis and over 95% of them not being secure, this is going to be a continuous catch-up battle. So, we need to be much more vigilant now than ever before.

About P20

P20 brings together industry leaders, government and regulators to collaborate on and develop solutions to non-competitive issues in the payments industry. Our vision is to create a more accessible, secure and inclusive payments ecosystem in which commercial competition can thrive in a safer environment for the benefit of all.

P20's key areas of focus are combating fraud & criminal transactions, cyber security and financial inclusion - and on a regular basis, we publish thought leadership and best practice reports on these issues.

Every September, P20 hosts its Global Payments Conference and brings together industry leaders, politicians, government officials, regulators, thought leaders and others to highlight trends, debate industry priorities and shape the future.

payments20.com
P20 - Payments 20
@P20payments