CISCO SECURE

Building Security Resilience

Stories and Advice from Cybersecurity Leaders

Cybersecurity professionals have dedicated their careers to protecting organizations and building resilience.

And today, that job is tougher than ever.

Organizations are operating as integrated ecosystems with boundaries between corporations, customers, suppliers and partners all blurring. We’re also adjusting to constantly shifting work patterns, and hybrid work is here to stay.

A focus on resilience has supercharged security concerns, raising difficult questions for today’s executives:

- When will threats hit us?
- Are we prepared to detect all of them?
- Where are we most exposed to risk?
- Can we mitigate effects quickly?
- How fast can we recover?
- Are we getting better?

This e-book features stories and experiences of security leaders from around the world, who discuss how they’ve integrated cyber resilience into their organizations.

They also offer guidance on which practices have the greatest impact on an organization’s ability to adapt to change.

What does security resilience mean to you?

Liz Waddell

Incident Response Practice Lead, Cisco Talos | LinkedIn | Twitter

For me, there are four key parts of what makes a company resilient. The most important thing is to invest in your people – protect their mental health, first and foremost. Security is an industry notorious for people being overworked and burned out. Make sure you have the right people in the right places. Invest in their training so they know your environment and technology and are ready to respond and protect it.

The second important thing is to align your business continuity and disaster recovery (BCDR) plans with your incident response plan. Doing this will mean recovery plans for your company are driven by your critical business needs. This alignment should result in knowing where your key assets are, what other systems they communicate with, and how they operate in your network.

The third strand is finding the easy wins which provide the maximum benefit for your organization when building your cyber defense strategy. These are things like multi-factor authentication (MFA), VPN, logging your passive DNS, and having response retainers in place – all things that most companies can put into place fairly easily.

Another example would be to consider having a direct security role reporting to your CEO or board and making sure that your board is educated on the risks happening in the world in terms of cybersecurity. That's important not only because they're funding your investments, but also because they need to understand what the risks are to the company.

The fourth and last part of the puzzle is to know your external risks. What are your risks from third parties and the supply chain? It's also important to have a situational awareness of the world. Events that are happening in the news, while perhaps not directly cyber-related, will have an impact on what you're protecting against.

What are some key considerations to building security resilience in your organization?

Richard Archdeacon

Advisory CISO, Cisco Secure | LinkedIn

Resilience requires the ability to manage change in such a way that the operations of the organization can still function. The change may be positive, for example, a new partner acquisition, or negative, such as being the target of a cyberattack.

The starting point for security teams has always been planning. Using a risk-based approach looking at the threat, the vulnerability, the probability, and the impact are all parts of the full risk equation. To understand the risk, potential scenarios are played out in the following way: Assume a threat exists, then assess the likelihood that it may affect us, and finally, examine how we can block any vulnerability and reduce the impact. Continuity and recovery plans are built around these scenarios.

Increasingly, CISOs are looking at how they can maintain a high level of continuity in the face of other nonthreatening changes. Balancing risk with opportunity, control and adaptability, such as managing the secure deployment of an external team of consultants, or ensuring a new supplier can be linked in to care for systems without increasing exposure is all part of a resilience profile.

> "The starting point for security teams has always been planning. Using a risk-based approach looking at the threat, the vulnerability, the probability, and the impact are all parts of the full risk equation."
>
> Richard Archdeacon | Advisory CISO, Cisco Secure

To achieve this, CISOs are preparing by:

1. Gaining support from leadership teams across their whole organization. This is not a technology or security issue, but a business challenge.
2. Developing board-level representation to champion resilience.
3. Ensuring that processes are in place and practiced by all stakeholders.
4. Continuing to develop both general threat intelligence and specific industry threat intelligence.
5. Introducing flexible technologies that provide clearer visibility across their assets and the centralized ability to implement new policies and controls.

Goher Mohammad

Head of InfoSec, L&Q Group | LinkedIn

Resilience is about taking a risk-based approach to what the business can tolerate. Together with the CIO, and/or the board, security leaders as the subject matter experts should clearly steer and articulate the risks; and what to do about them – thus enabling the organization to weigh up the correct decision.

If the cost of prevention is millions, but the total damage (if it happens), is only in the thousands, then that should be a factor in the decision and it would not be incorrect to accept the risk. However, it's not just about finances – it's also about reputation, and the long-term effect that a data breach might cause. All things should be considered, then try to reach a decision about what you can tolerate (and what you can't tolerate) as an organization.

Also, come up with a list of assets that you absolutely can't live without sometimes referred to as the crown jewels, as well as assets you can live without for a short period of time. And then layer your security based on that based on the threat model. It is not always possible or feasible to have the highest level of security on every single asset.

No CISO has an infinite budget or resources. You can't do everything and protect everything. And that's OK. You aim to protect what is most important to you as an organization and anything that touches that. Using this approach you build your resilience and continue to do so proactively as quickly as you can.

> "It's not just about finances – it's also about reputation, and the long-term effect that a data breach might cause."
>
> Goher Mohammad | Head of InfoSec, L&Q Group

Martin Lee

EMEA Region Lead, Strategic Planning & Communications, Cisco Talos | LinkedIn

Resilience means being able to manage the threats that we face, and not immediately crumbling when a threat succeeds in causing harm. Resilience is achieved through combining protection with incident response planning.

The first step in becoming resilient is to be aware of threats that we face. You can't take steps to protect yourself if you have no idea of the nature of these threats. The foundation of successful resilience comes from understanding the threats and your own weaknesses.

Armed with this knowledge, you can implement protections to reduce the likelihood that threats will affect you, and ensure that if a threat does succeed, that the effects will be minimized.

However, we must accept that no protection can ever provide complete coverage, nor can we fully anticipate how threats may change and evolve. Hence, we need to prepare ourselves to respond swiftly and effectively when a threat impacts us.

Making sure that our systems have no single points of failure helps ensure that operations can continue even if one component has to be taken out of action due to a threat. Planning and rehearsing our responses to incidents allows us to remediate threats and restore normal function as soon as possible.

> "The foundation of successful resilience comes from understanding the threats and your own weaknesses."
>
> Martin Lee | EMEA Region Lead, Strategic Planning & Communications, Cisco Talos

Lidia Giuliano

Information Security Professional | LinkedIn | Twitter

As a security advisor, one thing I look at in order to evaluate resilience is where an organization stands with practices such as data classification, and identity and access management. The overall holistic design of these areas needs to be examined from a security perspective to see if they are sound.

One of the most effective ways to achieve resilience in any organization is to take a team approach, even if it is an informal team – a collaborative environment, rather than an established corporate grouping.

This is important because a person is never alone in this endeavor.

For example, if I am working with developers, they need to be keenly aware that part of the responsibility of developing an application is not just functionality, but security – that is, making the application safe for our customers to do business with us.

Making sure that the organization shares the vision and actions of good security requirements is what will propel resilience; and ensuring that penetration testing, code scanning and data classification are all done at the appropriate time.

What I love is seeing the ways that security professionals are actually helping projects. It's a different aspect than how security was traditionally treated. Communication with the security professionals is helping the business to design security into the project at the start. And that builds resilience by eliminating the scramble to bolt security on later, especially after an incident is discovered.

> "One of the most effective ways to achieve resilience in any organization is to take a team approach, even if it is an informal team – a collaborative environment, rather than an established corporate grouping."
>
> Lidia Giuliano | Information Security Professional

James Packer

Head of Information Security | LinkedIn

One of the areas where it's crucial to proactively invest time is in the ability to get accurate and actionable threat intelligence in the right context. This can be very difficult because there are many different vendors and tools available that deliver very detailed threat intelligence, but often what they fail to do is make that information relevant and bring in a broad context. For example, the current turmoil in the world makes it important to anticipate cybercrime from a geopolitical standpoint.

Being able to show context adds real value to the business. If you can show executives how you account for the threats to your service delivery, operations and critical functions based on what's going on in the real world, then they can see the importance of what you are doing. That gives the leadership meaningful confidence that your business is in the resilient state.

An important aspect of resilience comes with focusing on activities that actually align with what the business does. It's all well and good to try to conduct exercises to test your resilience, but with the new work models that have emerged in recent years, the exercises outlined in a variety of frameworks may not be the most valuable thing to be doing right now.

A better approach may be to pay attention to where others have fallen victim recently, and try to make sure that the resilience activities you're undertaking are aligned to what is going on in the real world, focusing on those things that are most likely to impact your industry, and specifically your organization. It gives you a real-world test of resilience.

James Packer (Continued)

Head of Information Security | LinkedIn

To take that idea further, ransomware is very prevalent, but how do you test resilience against ransomware? The value comes in by looking at the ransomware types that most organizations are being hit by. Are those ransomware variants targeting specific sectors and specific organizations? How does that then apply to you, and how can you model your resilience exercises to answer those real-world scenarios using what has happened to similar businesses?

Too often, there is a very clear disconnect by the business. With ransomware, you may be running a resilience exercise, and some of the business teams may not have a technical understanding of the systems, what ransomware is, and its impact to their workflow. But, when you show that a service can be rendered unavailable, or that data may be stolen and extorted, then the stakeholders that are involved in those resilience activities can get an accurate view to understand how it would materially hurt the business.

Alternatively, they may determine that certain functions can be halted for a short period without harm to the business. These types of resilience activities add a lot of value by building that clear connection between the business and the technology.

> "It's all well and good to try to conduct exercises to test your resilience, but with the new work models that have emerged in recent years, the exercises outlined in a variety of frameworks may not be the most valuable thing to be doing right now."
>
> James Packer | Head of Information Security

Corien Vermaak

Cybersecurity Architect, APJC Region Center of Excellence, Cisco

LinkedIn | Twitter

Resilience is far bigger than just security, but of course, security is such a key part. Security is like the king piece on the resilience chessboard. If our processes topple over and never recover, the game is over. And yet – we're surrounded by other disciplines, who have their own moves they need to make to protect the organization as a whole. There's a lot to protect, and with limited moves, we need to be very calculated. And that's why we're seeing a big move towards risk-based security.

For example, I might have a server that doesn't have critical information within it. But the server has a known vulnerability that needs to be patched. It's a back-end server that we use for DevOps. You have the same server, with that same vulnerability, but it's internet-facing, and it has customer data on it. Our risks are different, even though it's the same vulnerability. The need to patch is a far bigger priority for you.

In a world where we can only do so much, we need to focus on the things that matter. Address the critical issues first, and then make a plan to address the other vulnerabilities you might be exposed to. To do that, you need accurate, prediction-based threat intelligence, based on your uniqueness as an organization. This priority-based resilience building will address a lot of security operational issues that we've seen in the past.

> "In a world where we can only do so much...Address the critical issues first, and then make a plan to address the other vulnerabilities you might be exposed to."
>
> Corien Vermaak | Cybersecurity Architect, APJC Region Center of Excellence, Cisco

Cisco SECURE

Motor Oil Group's 6 pillars to security resilience success

Christos Syngelakis

CISO and Data Privacy Officer, Motor Oil Group | LinkedIn

MOTOR OIL

Motor Oil Group is an oil refinery company with 50 years of history, and subsidiaries operating in the oil retail and renewable energy sectors in the countries of southeastern Europe. In an organization with such a diverse infrastructure and business, when it came to cyber resilience, the biggest challenges to address were legacy systems and mindset.

As our board has been heavily investing in digital transformation over the past five years, the security goals were production resilience, and the minimization of brand impact and exposure in case of a technological incident. It is part of critical national infrastructure, and any interruption can have broad consequences.

> "Moving towards strategic partnerships with vendors simplifies our complexity and maximizes the return on investment from every solution. As an example, a cloud service provider is our partner, ensuring scalability and future-proofing further expansion to the cloud."
>
> Christos Syngelakis | CISO and Data Privacy Officer, Motor Oil Group

The following are the pillars of Motor Oil's security strategy to proactively anticipate threats, build cybersecurity resilience, and effectively support the business:

1. **Leadership buy-in** – The CISO reports to the organization's CEO. Business goals and objectives are aligned with cybersecurity plans to ensure maximum return on investment and effectiveness
2. **Recognize the problem area** – It all starts with recognizing where your weaknesses are. Self-awareness is important in critical infrastructure such as oil refineries. Knowing ourselves and our strengths and weaknesses has helped us to be five years ahead of the competition and demonstrate five years of efforts and progress in changing the corporate mindset.
3. **Invest in humans** – Humans are the most important part of the change.
4. **Converge information security with operational technology** – Have these two domains listen to and respect each other. They are both working for the same common goal, therefore, it is important to speak the same language.
5. **Implement "security by design"** – Protect digital transformation initiatives and migration to the cloud. For example, data analytics for predictive maintenance is now done in the cloud, which could expose very critical systems to various threats and vulnerabilities. The goal is to build a security perimeter in a perimeterless world without imposing any overhead, and without any false positives. In our industry, false positives are equal to danger.
6. **Identity management** – Use multi-factor authentication as the preferred choice whenever it can be integrated with our systems.

I want to end by acknowledging that one of the biggest challenges for CISOs is burnout. In an always-on environment where there is always something new to learn, as well as a tremendous expansion of technology and requests for new projects, the challenge of finding balance is one of the top issues. This brings me back to point three above – invest in your people and prioritize their mental health.

How can security resilience proactively enable organizations?

“Accidental CISO”

Twitter

First and foremost, people and relationships are key to information sharing when it comes to anticipating threats to operational resilience. Other groups in the organization know their areas better than my team ever will.

They also know what the business impact will be. Labeling “happy path” thinking has been very helpful to get the team to step back and consider what doomsday scenarios would wreck their plans and make it impossible for them to operate.

We established standard design patterns and team norms to mitigate those doomsday scenarios. Design patterns can be in the form of standardized technical architectures, requirements or operational processes. Team norms are usually in the form of cross training, established roles, modes of communication and escalations.

The biggest benefit from our proactive approach was realized in March of 2020, when the company was forced to go fully remote, indefinitely, on short notice. In 2019, due to conversations with other teams across the organization, we had realized that we had four big problems with our IT infrastructure that would severely limit our resilience.

1. Many critical business processes depended on IT infrastructure that was housed at the office where we lacked power, internet and cooling redundancy.
2. Managing the IT infrastructure, especially the corporate telephone system, required specialized skills that we didn’t have internally. We were heavily reliant on external resources to help us manage the equipment; and in the event of a problem, we were unsure how quickly we would be able to restore service.

3. We didn’t have the team necessary to monitor and secure our internal IT systems sufficiently, and the managed service provider was not up to the task.
4. Remote access provided poor experience for customer-facing phone calls.

To address the risk of extended outages and the need for a better remote work experience, we made the decision to migrate all our internal IT infrastructure to cloud-based services. When the shift to full-time remote work happened, we weren’t caught unprepared.

Christos Sarris

Lead Information Security Analyst, Sainsbury's | LinkedIn

From my years in the medical sector, I witnessed how security resilience can enable an organization. In particular, when my team had to deal with a very sophisticated malware strain that was designed to target a specific brand of widely used intensive care units (ICUs).

ICU medical devices (ICUMDs) are used to closely monitor, stabilize, and treat ICU patients who are often unconscious and rely almost solely on these devices to survive, and the malware affected the syringe pump (used to administer a specific quantity of medicine) and the pump monitoring functionality that could result in threat of life.

When we assessed these devices, we identified both current security weaknesses and future threats. It became clear to us that we needed to handle key areas like software updates, patching and access with a very different approach than with other IT-related devices. We implemented a very refined process across the Identify, Detect, and Response phases of our security resilience strategy.

In doing so, we identified the malware in an isolated testing environment. It was revealed that the malware was introduced through a compromised patch that was released by the vendor. At that time, no endpoint protection software was able to detect this malware, and if we followed the typical security processes, we would have placed the lives of hundreds of patients in danger. No one ever thought that someone would design something so malicious that could cause the loss of life.

For many security professionals who work on the front lines, security resilience indicates the ability of an organization to adapt to known and unknown threats. Nonstop business transformation at the time of a crisis is a key strategy for building enterprise resilience.

> “For many security professionals who work on the front lines, security resilience indicates the ability of an organization to adapt to known and unknown threats.”
>
> Christos Sarris | Lead Information Security Analyst, Sainsbury's

Nigel Sampson

Head of Cybersecurity, International Data Group (IDG) | LinkedIn

Procuring solutions is just one part of the trilogy of People, Process, and Technology. Having staff to support the solutions is just as critical. Often, organizations fail to keep their cybersecurity staff because they have no current salary data, and have no way to understand the exponential growth of those individuals in the field and their market value. There needs to be a closer relationship between cybersecurity, finance, and HR in order to build and support security programs.

In a prior role, implementing a flexible, modular GRC was the most impactful solution. However, what made it effective towards gaining interest from multiple departments was the ability to be cross-functional, covering vendor management, vendor risk management, policy management and IT risk management. It provided a centralized solution for risk management, but also provided a repository for the enterprise policies.

In providing a vendor management solution, it also provided a vendor risk management solution where critical vendors could be risk-ranked. Risk profiles for individual vendors could then be determined, as well as the overall third-party risk profile. The cost/benefit of such a solution is easily justified when reviewing the manual processes included in each of the use cases.

The GRC solution started off with one module and, over time, expanded to four modules with other departments seeking access in order to centralize their documentation or to use it for their core processes.

> "There needs to be a closer relationship between cybersecurity, finance, and HR in order to build and support security programs."
>
> Nigel Sampson | Head of Cybersecurity, International Data Group (IDG)

Haroon Malik

Security Consulting, Director, NTT Data | LinkedIn

A couple of years ago, I worked with a retail company that had huge risks with their third-party supply chain. Supply chain attacks have been a popular method of attack recently. However, this is not a new phenomenon, and I was called to help that company after it had quite a big data breach. The breach was not a result of their own defenses, but a weakness in one of their primary suppliers.

I led a third-party supplier review, assessing areas such as who were their critical suppliers (they had about 200 suppliers). Then, we needed to examine which ones they were exchanging personal and confidential data with. We then proceeded to break all the suppliers into tiers, based on the classification of information.

We then audited all the tier-one suppliers. The way that helped the client was that it gave them a truer understanding of which of their suppliers were risky. As a result, we saw a marked improvement in the way that the company chose their suppliers. It wasn't just based on the quality of goods; it was based on security principles as well.

Another important piece of resilience is the ability to not only identify when something isn't quite right, but also do it quickly. These are concepts known as mean time to detect (MTTD), and mean time to respond (MTTR).

Threats exist and incidents happen. Resilience is achieved when both the likelihood of an incident occurring is reduced, and the impact caused is minimized.

> “Threats exist and incidents happen. Resilience is achieved when both the likelihood of an incident occurring is reduced, and the impact caused is minimized.”
>
> Haroon Malik | Security Consulting, Director, NTT Data

Ian Thornton-Trump

Chief Information Security Officer, Cyjax Limited | LinkedIn | Twitter

Working in the cyber threat intelligence (CTI) industry in the UK is always going to require an elevated alert level. Fortunately, we have architected our infrastructure in such a fashion as to reduce the attack surface and exposure of vulnerable services.

This commitment to "best practice" architecture also provides a comfortable degree of resilience. For us, it's all about having knowledgeable developers who pride themselves on the creation of secure code and ensuring it's properly deployed with rigorous adherence to ISO 27001 compliance.

As a nearly virtual company, our data and email are all contained within Software-as-a-Service (SaaS) clouds for the ultimate in accessibility and data protection provided by those top-tier providers. Working in the CTI world, everyone in the company is acutely aware of the threats that all organizations face, including our own.

We have a chief compliance officer who works with us, and all layers of the company work against threat actors in the physical and virtual world on a daily basis. This promotes a strong security culture, as well as effective resilience.

> "For us, it's all about having knowledgeable developers who pride themselves on the creation of secure code and ensuring it's properly deployed with rigorous adherence to ISO 27001 compliance."
>
> Ian Thornton-Trump | Chief Information Security Officer, Cyjax Limited

Michelle Dennedy

CEO, PrivacyCode, Inc. | LinkedIn | Twitter

One example of building resilience is from my days as Cisco's first chief privacy officer. When it came time to draw up contracts, we measured a pattern of distrust and confusion when customers wanted to buy collaboration or other privacy sensitive products. Long negotiations covered basic questions such as "Where is data stored?" and "Who manages the sign-on data about our employees and customers?"

I was at the London Transport Museum exhibit when the solution hit me: the simplicity of the maps to the London Underground was perfect! What if we could show customers what data was in question, and where and for how long, in a simple to digest infographic?

That's what we created and published in the Cisco Trust Center, and the results were immediate, measurable and lasting. When people can visualize systemic, complex issues, they can plan, commit and build together.

My current company is PrivacyCode, Inc. We provide a platform that allows stakeholders who must create and enforce complex legal and policy requirements to effectively translate them into consumable, measurable and action-oriented tasks for technical teams.

In a world with constant change and growing complexity, clearly communicated and granular-level leadership creates and reinforces resilience. I am always seeking simple and easy-to-engage steps to solve monumental challenges.

> "In a world with constant change and growing complexity, clearly communicated and granular-level leadership creates and reinforces resilience."
>
> Michelle Dennedy | CEO, PrivacyCode, Inc.

Additional resources

As our experts have stressed, when everything is open and connected, security resilience requires more than what past approaches have offered.

The old methodology of siloed security, which was focused on treating all threats equally, is making way for a new form of security resilience: the drive towards adaptability and constant verification while always considering the context.

Another common theme amongst our contributors is that humans are absolutely key to building resilience. Protecting their mental health, and reducing the risk of burnout, is more important than ever. For expert tips and resources on this topic, read our e-book: Creating Safe Spaces: Leaders and Practitioners on Mental Health and Avoiding Burnout.

> **"You aim to protect what is most important to you as an organization and anything that touches that. Using this approach you build your resilience and continue to do so proactively as quickly as you can."**
> Goher Mohammad | Head of InfoSec, L&Q Group

Learn how you can empower your business to withstand today's unpredictable threats and emerge stronger tomorrow.

Visit: cisco.com/go/security-resilience

Thank you for reading

Building Security Resilience

Stories and Advice from Cybersecurity Leaders