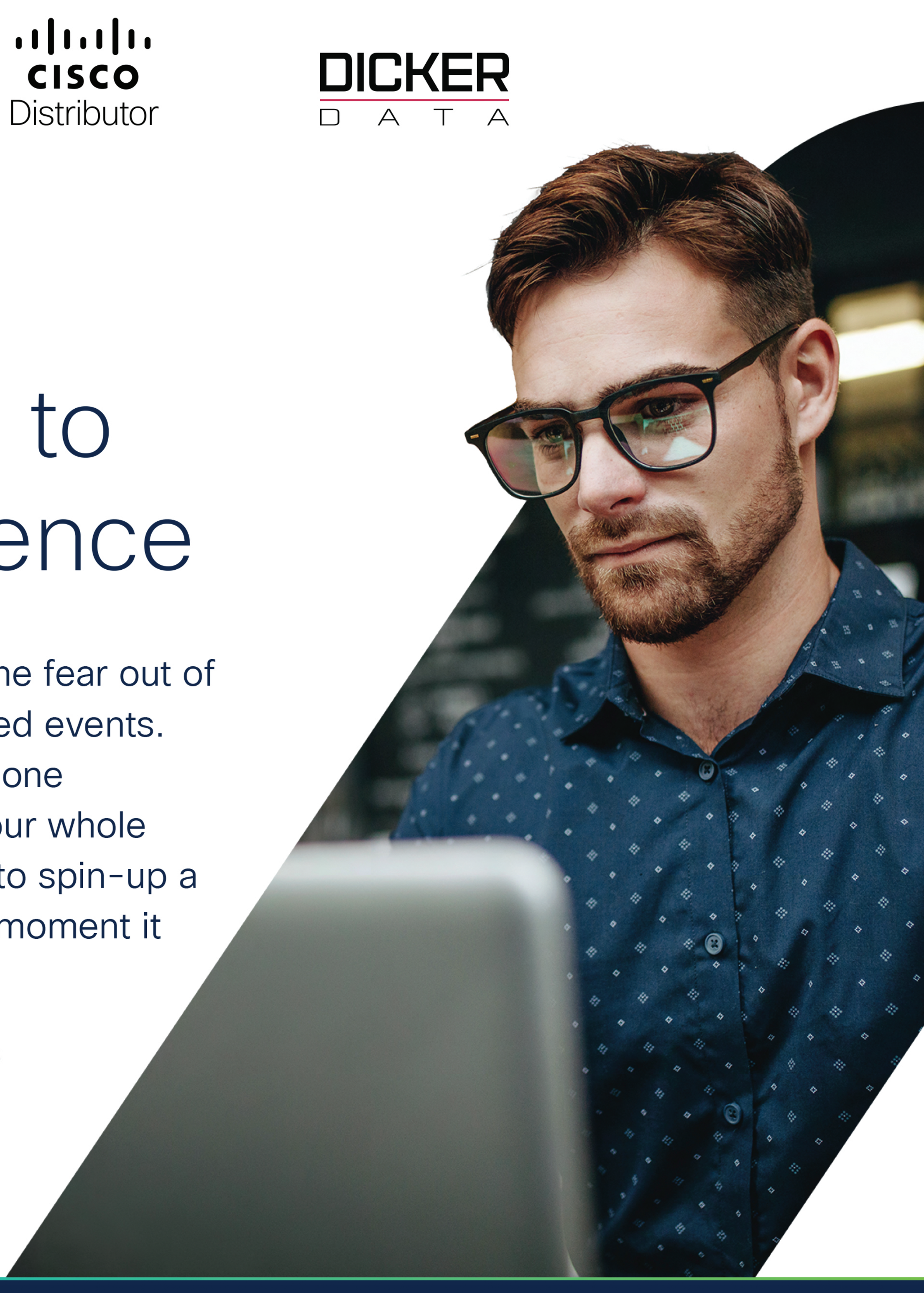
CISCO SECURE | CISCO Distributor | DICKER DATA

5 key steps to security resilience



Security resilience is about taking the fear out of change, and planning for unexpected events. When you have security resilience, one accidental click won't jeopardize your whole company. Or if you suddenly need to spin-up a branch office, it can be secure the moment it goes online.

So, what are the key steps towards security resilience?

1 Fostering a culture of security

In a strong security culture, employees are treated as part of the solution rather than the problem. Awareness of the role they play is key. This may be seen by regularly reporting phishing attempts, potential malware, and other incidents. Conversely, frequent security policy violations and workarounds are evidence of poor security culture.

46% Organizations that foster a culture of security see a 46% increase in resilience.

Source: Cisco Security Outcomes Report Volume 3

2 Develop executive level representation

Organizations that report poor support from top executives show security resilience scores that are 39% lower than those with strong backing from the C-suite.

The security team can't solely be responsible for security resilience. There should be buy-in at the top.

So how do you develop executive level representation?

- Understand what executives care about
- Explain how your resilience plan contains business focused outcomes
- Clearly communicate the risk of doing nothing
- Discuss what risks you are comfortable with taking, and what you're not comfortable with

3 Have your resources in place

Maintaining excess internal staff and resources in order to better respond to unexpected cyber events makes a big difference.

If maintaining extra staffing to handle unexpected events isn't feasible for your organization, firms that retain external incident response (IR) services show an 11% average improvement in security resilience. Consider getting those retainer contracts in place with a credible IR service provider so help is just a phone call away.

15% Organizations able to maintain excess resources achieve 15% higher security resilience scores on average than those without "flex" resources to tap into when needed.

Source: Cisco Security Outcomes Report Volume 3

4 Utilize threat intelligence as part of your detection and response capabilities

Detection and response capabilities work best when they know what to look for and how to find it. Many look to quality cyber threat intelligence for that purpose.

No protection can ever provide complete cover, and we can't fully anticipate how threats may change and evolve. Preparation is key. Ensuring that systems have no single points of failure helps ensure that operations can continue even if one component must be taken out of action due to a threat.

There are two key pieces to a cohesive Extended Detection and Response (XDR)e solution:

- Cyber threat intelligence
- Automation/orchestration

Organizations with these capabilities boasted a 45% better overall resilience score than those without a XDR solution.

5 Focus on simple to manage, flexible technologies

Good news: there's no difference in security resilience outcomes between heavy on-premises versus heavy cloud environments. Neither is "better" than the other when it comes to security resilience.

However, keeping things simple and friction free is a key success factor for both types of infrastructure.

Multi Factor Authentication (MFA) is one of the best ways to make your organization more resilient and can be simple to roll out and manage.

11% Deploying MFA can boost security resilience scores 11%.

Source: Cisco Security Outcomes Report Volume 3

To learn more, read our eBook:
Your guide to building security resilience, with Cisco Secure

Cisco Secure is helping organizations everywhere prepare for the unexpected. Not so they can avoid it. But so they can face it, quickly adapt, and withstand it.

CISCO The bridge to possible