The Human Side of Cybersecurity

Imagine the Worst-case Scenario.

Your entire datacenter has been shut down by a sophisticated ransomware attack. Sales, customer service, and finance are unable to operate. You're a senior IT leader, in charge of restoring the systems, but finding a solution has proved elusive.

Your team, which was already short-handed, has been working weeks on end with very little breaks or time off. Some practitioners have ***clocked as much as 36 hours straight*** without sleep. You're getting concerned that fatigue is leading to poor decision making, potentially risking the recovery effort itself.

You desperately need additional resources that can immediately jump in and help address the problem, but where to find them?

This scenario might sound like the start of a novel, but it's based on the real-life experiences from Dell customers. It highlights a significant problem in today's cybersecurity environment: The Human Element.

Recent data indicates that the industry suffers from a shortage of nearly 5 million security professionals. While the resource needs are felt most acutely during an incident, the solutions begin much further upstream.

Start with Building and Growing a Talent Pipeline

The first step to ensuring you have the resources you need is to build a talent pipeline:

College recruiting and internships

Engaging with local universities and technical schools can unlock a steady stream of junior talent. These individuals can be nurtured into high-impact team members over time.

Ongoing training and development

While time and budget are under constant pressure, cybersecurity professionals must keep up with changes to both tools and threats.

Focus on retention

Good practitioners are in high demand, especially if they have experience navigating an attack. If you don't retain your top talent, someone else will.

Even a strong team may not be enough to handle the stress of managing through an attack, so plan ahead by identifying additional support before it's needed:

Evaluate third-party resources

Cybersecurity consulting and staff augmentation firms can assist your team during both ongoing operations and incidents. Build relationships with those companies, even if you don't need them now, so you have access to those resources when needed.

Dell offers a number of services that can augment existing teams, including virtual CISO (vCISO), incident response, and cybersecurity advisory.

Leverage AI

Take advantage of new AI capabilities being built into cybersecurity tools such as log analysis, anomaly detection, triage of low-level alerts or specialized training to help met resource gaps and address operational needs, potentially freeing up team members to focus on higher-order tasks.

Resources Challenges Are Greatest During a Cyberattack

As the initial scenario illustrated, a major cyberattack can cripple your organization, paralyzing major systems and business operations. Every minute costs the company money, and the cybersecurity team will face tremendous pressure to fix the problem.

Ensuring that your teams are as up to date as possible will have a direct impact on incident response and related stress on the team.

Keep in mind that training must extend beyond the security pros to all employees, as they are the first line of defense.

This story underscores a central challenge: the cyber defenders are ultimately human. They have limits, and when those limits are exceeded, even the strongest professionals can fail. Mental fatigue, stress, and burnout are now critical factors in cybersecurity posture.

While there may be no single solution to this challenge, the following strategies can go a long way:

Building a strong team and talent pipeline

The most fundamental solution to this problem is to not let it become an emergency – build a strong team with redundancies in place.

Planning for the human side of an attack

Incident response plans are critical, and they MUST include plans for managing staff, scheduling, and handling employee downtime.

Leverage third-party resources

External cybersecurity consultants can help augment your team. Dell's incident response services, for example, can have an expert team on-site within hours—ready to assess, contain, and begin remediation immediately. We have helped many customers make it through cyberattacks.

AI Can Help, But It's Not a Silver Bullet

AI offers tremendous promise to enhance cybersecurity tools and programs. Its capabilities will ultimately run the gamut from predictive analysis to developing tailored training programs to even proactively addressing threats before they spread.

Perhaps even more importantly, AI can provide defenders a real-time support system during an incident. Machine learning models trained on historical attack data can recommend actions based on similar past events.

As natural language processing makes its way into cybersecurity tools, analysts will have the ability to interface directly with their systems, identify threats, and deploy solutions.

AI can also monitor behavioral patterns to flag when a human analyst might be making repeated mistakes – perhaps due to exhaustion – and prompt a shift change or a set of fresh eyes.

While cybersecurity tools are rapidly integrating more sophisticated AI tools, many of the most powerful capabilities are still in development. Keep in mind that as of now, AI cannot replace the skills of an experienced practitioner, ***especially one who has been through an attack before***.

Recommendations to Take Advantage of AI:

Understand how the tools can help your security operations

Do a detailed analysis of AI tools and implement them where they can be most effective. Potential easy wins include advanced threat detection, automating repetitive tasks, and using AI in identity management.

> "Having a partner who does incident response, remediation, and recovery on retainer is a best practice."
>
> ***Jason Rosselot***
> *VP, Cybersecurity and Business Unit Security Officer, Dell Technologies*

Plan for AI's future

Understand when new capabilities are coming available, how they will benefit your team, and develop a plan to implement them.

Incorporate AI into workforce planning

As automation reduces manual tasks, the composition of your security team may need to evolve. You may need higher level resources to analyze and act on security information, versus compiling it. Adjust your hiring and development strategies accordingly.

AI will become a significant part of your cybersecurity operations, if it hasn't already. But keep in mind that there is no substitute for a skilled and experienced practitioner. The goal should be to use AI to automate operations and make the human resources more effective, ultimately preventing attacks and minimizing their impact when they occur.

Advance Cybersecurity Maturity: One Step at a Time

Like everything in cybersecurity, addressing the human element is a journey, not a destination. Incremental effort and even small steps toward progress make a difference and add up over time. The important thing is to remember that even the best technology and security tools are ultimately only as good as the people running them.

DELL Technologies

Dell products and solutions that can help

Featured Dell Solution	Description
Incident Response Services	A team of industry-certified cybersecurity experts standing by for swift response in the event of a cyberattack. We work side by side with you to eliminate the threats until normal operations have resumed.
Cybersecurity Advisory Services	Expert guidance that can help you find and address blind spots in your security strategy, protect your assets and data, and enable continuous vigiliance and governance.
vCISO	Virtual Chief Information Security Officer and cybersecurity expert who can assist in identifying and managing risk as well as guide strategic decision making.
Managed Detection and Response	Reduces manual efforts and streamlines day-to-day security operations by providing monitoring, threat detection, investigation, and rapid response across endpoints, network, and cloud.. Customers choose their preferred XDR platform (Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR or Microsoft Defender XDR) and receive expert guidance, quarterly reports, and up to 40 annual incident response hours.

Learn how to address some of today's top cybersecurity challenges at **dell.com/cybersecuritymonth**

DELL Technologies