Unarmed and Unprepared†

When most organizations plan their cybersecurity programs, they focus on detection and response capabilities. In reality, a comprehensive approach requires an organization to be prepared for all cybersecurity threats, including those that require human intervention. The AT&T Cybersecurity Risk Readiness Assessment can help organizations better understand the gaps in their cybersecurity postures.

People Problems

IT organizations face challenges when it comes to human elements of cybersecurity. Policies and processes are only part of the problem. Human elements are also at play. Just look at phishing, which continues to be one of the most effective ways to penetrate an organization. But how many company’s test their employees’ awareness of phishing? Less than a third.

Budget shortfalls may be to blame in both cases, keeping IT teams from procuring the tools and services they need. A mere 6% of respondents say they have confidence in their security budget and resources. They also feel there’s a long way to go. AT&T is here to help, offering a full stack of security solutions. By integrating people, processes, and technology in a focused effort to help strengthen your cybersecurity posture, AT&T has the tools and services to help your organization prepare for any threat.

Spur-of-the-Moment Security

An effective cybersecurity program includes comprehensive threat tolerances and incident response plans that address potential vulnerabilities. An organization’s cybersecurity program must focus on both human and technology elements, as well as being designed and implemented with speed in mind. The AT&T Cybersecurity Risk Readiness Assessment can help organizations understand how their incident response programs stack up. Or download the full AT&T & Readiness Assessment to find out how your organization stacks up. Or download the full AT&T Cybersecurity Risk Readiness Assessment full stack of security solutions. By integrating people, processes, and technology in a focused effort to help strengthen your cybersecurity posture, AT&T has the tools and services to help your organization prepare for any threat.

Which element of human security do you test? Of those who said they tested elements of human security, 49% said they do it once a year, 17% twice a year, and 14% multiple times a year. When asked to describe their organization’s cyber-security program, a full half of respondents said their policies were “ad-hoc.” As for incident response coordination capabilities, a whopping 71% described those as not up-to-date policies as well as detection and response capabilities. But many are left out of the loop, making security an afterthought in the deployment process.

What is your cybersecurity playbook? Of those who said they had an incident response playbook, 50% said it’s well-defined but not up-to-date. Another 23% said that it’s well-defined but not for detection and response. A security information and event management (SIEM) tool can help organizations efficiently manage the data generated during an incident. However, many organizations are not using SIEM to its full capabilities or—as 63% of respondents stated—are not using it at all. The same goes for penetration testing—almost half never do it. For analysis, but not for detection and response coordination capabilities, a whopping 71% described those as not integrated. There’s no reason to spend energy on developing and deploying a security program that’s not going to be effective when you need it. Spur-of-the-Moment Security

Unarmed and Unprepared†

AT&T: Full-Stack Security

Which area of cybersecurity do you feel is not integrated, to learn more.

AT&T: Full-Stack Security

Unarmed and Unprepared†

People Problems

Which element of human security do you test? Of those who said they tested elements of human security, 49% said they do it once a year, 17% twice a year, and 14% multiple times a year. When asked to describe their organization’s cyber-security program, a full half of respondents said their policies were “ad-hoc.” As for incident response coordination capabilities, a whopping 71% described those as not up-to-date policies as well as detection and response capabilities. But many are left out of the loop, making security an afterthought in the deployment process.

What is your cybersecurity playbook? Of those who said they had an incident response playbook, 50% said it’s well-defined but not up-to-date. Another 23% said that it’s well-defined but not for detection and response. A security information and event management (SIEM) tool can help organizations efficiently manage the data generated during an incident. However, many organizations are not using SIEM to its full capabilities or—as 63% of respondents stated—are not using it at all. The same goes for penetration testing—almost half never do it. For analysis, but not for detection and response coordination capabilities, a whopping 71% described those as not integrated. There’s no reason to spend energy on developing and deploying a security program that’s not going to be effective when you need it.

Spur-of-the-Moment Security

Unarmed and Unprepared†

AT&T: Full-Stack Security

Which area of cybersecurity do you feel is not integrated, to learn more.

AT&T: Full-Stack Security

Unarmed and Unprepared†

AT&T: Full-Stack Security

Unarmed and Unprepared†

AT&T: Full-Stack Security