Red Hat

Cybersecurity

The cost of human error

Humans make mistakes, particularly when resources are stretched. Yet there is no room for error when it comes to cybersecurity. In this piece, we examine the problem and how automation can help.

The cost of cybercrime

Cyberattacks are increasing, and companies are paying the price.

67,500

reported cyber attacks[1]

1 report of a cyber attack **every 8 minutes**

US $33 billion

in self-reported losses[1]

13% growth

in the number of attacks, year over year[1]

The role of humans in cyber incidents

Too often, human error and oversights expose gaps in security, leading to cyber incidents.

US$3.33 million

The average cost of a data breach resulting from human error.[2]

> **"The weakest link in cybersecurity continues to be humans."**
>
> CompTIA, State of Cybersecurity 2021

80% of data breaches are linked to compromised privilege credentials[3]

Poor passwords

Passwords are the first layer of protection, yet they can be a weakness if your employees are using common passwords or the same one on every account.

Falling for scams

Phishing works. These scams prey on the fact that people are busy. But just one unwitting click from an employee could harm your entire system.

Slow patching

Every time a software company discovers a vulnerability, they fix it and release a patch to protect users. If you do not apply the patch quickly, your system is vulnerable.

Fixing firewalls

Firewall rules should be regularly reviewed. Plus, if you do not update your firewalls every time a new security update or patch is released, you are exposed.

Oversharing privileges

Humans can make errors in judgment and grant too many people administrator privileges. If access is overshared, your system is exposed to greater risk.

Forgotten backups

If your system backups are manual, your data could be vulnerable to human error. If systems fail or you lose a laptop, sensitive data could be lost.

Automation reduces the risk of human error

By automating key security tasks like patching, backups, and remediation, you reduce the risk of human error, and you will likely also reduce the cost of data breaches.

42%

gain in employee efficiency when network security is automated[3]

US$2.9 million

Average cost of a breach in organizations that have fully deployed security artificial intelligence (AI) and automation[4]

That's a 57% cost difference.

US$6.71 million

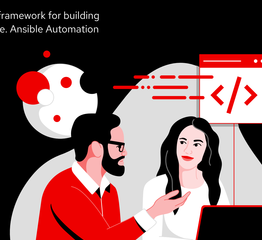
Average cost of a breach in organizations that do not use security AI and automation[4]

Red Hat helps automate your cybersecurity practice

Red Hat® Ansible® Automation Platform provides an enterprise framework for building and operating automation at scale, from hybrid cloud to the edge. Ansible Automation Platform allows users across an organization to create, share, and manage automation—from development and operations to security and network teams.

With Ansible Automation Platform, you can automate previously manual cybersecurity processes, which help mitigate the risk of oversights caused by human-based constraints.

To learn more, contact Red Hat today. >



1. Australian Cyber Security Centre. "ACSC Annual Cyber Threat Report 2020–21." Sept. 2021. **2.** IBM. "2020 Cost of a Data Breach Report." 2020. **3.** IDC White Paper, sponsored by Red Hat. "The Business Value of Ansible Red Hat Automation Platform." Doc #US48678022, Oct. 2021. **4.** IBM. "2021 Cost of a Data Breach Report." 2021.