Red Hat

Next

Security spotlight: The cost of human error and the advantages of automation

Why government agencies are reconsidering manual approaches to managing security and how intelligent automation helps prevent potential threats from costly security gaps

In this e-book:

01 Introduction: The growing threat of cybercrime

Cybercrime is on the rise. Last financial year, the Australian Cyber Security Centre (ACSC) received over 67,500 reports of cybercrime—a rise of 13% year on year—with self-reported losses totalling over $33 billion.[3] Of these incidents, roughly one quarter of them affected entities associated with Australia's critical infrastructure.

As government agencies embrace new technologies and adapt to hybrid models of work, cyber attackers are transforming their capabilities, too. Workforces and computing resources are becoming more distributed, and the rapidly evolving landscape of IT infrastructure presents bad actors with new opportunities to exploit security gaps and vulnerabilities—causing the organizational cost of data breaches to grow. Even an organization that develops a strong security posture faces more risks in this environment.

Proactive security against cybercriminals

As cybercriminals devise new ways to breach protected systems and data, organizations are facing internal and external pressure to develop more strategic and proactive protections against cyberattacks. In fact, their data security and privacy measures must comply with more comprehensive rules and regulations.

For example, the New South Wales (NSW) Cyber Security Policy now mandates the implementation and provision of a maturity assessment against the ACSC Essential Eight risk mitigation strategies.[1] And the Security Legislation Amendment of Australia's Critical Infrastructure Bill potentially increases the regulatory burden on government organizations that manage or operate critical infrastructure.[2]

Reinforcing your defenses

Organizations looking to improve their cybersecurity need to identify existing vulnerabilities first. Too often, human error and poor training can compromise security, even when comprehensive strategies are already in place. Left unchecked, small mistakes can introduce risk to your systems, compounding an already complex problem. As a result, organizations are adopting automation to increase reliability and reduce risk in their security strategy.

In this e-book, we'll explore how the risks introduced through human error affect the fight against cybercrime. We'll also discuss how automating key cybersecurity risk mitigation strategies can strengthen your security while reducing the volume of time-consuming tasks that burden your IT teams.

The cost of cybercrime in Australia.

67,500

Reported cyberattacks[3]

$33 billion

In self-reported losses[3]

13%

Growth in number of attacks, year over year[3]

1. Government of New South Wales. "DCS-2021-02 NSW Cyber Security Policy." Feb. 2021.
2. Parliament of Australia. "Security Legislation Amendment (Critical Infrastructure) Bill 2021." 2021.
3. "ACSC Annual Cyber Threat Report 2020-21." Australian Cyber Security Centre, Sept. 2021.

02 Effective security strategies should involve everyone

Humans make mistakes

Even within IT teams, people often underestimate or misunderstand their system's vulnerabilities and the resulting security risks. Our inability to accurately assess risk can result in significant costs to organizations.

For example, imagine this: A technician manually updates a firewall. They make one small mistake—which they don't perceive to be a problem—so the vulnerability goes unaddressed. What they don't realize is that this tiny error introduces a critical vulnerability into the organization's IT system, an opportunity that cybercriminals quickly take advantage of.

In this scenario, the technician's small mistake could result in various negative outcomes, including compromised data, violation of industry and government data security regulations, service interruptions, and system downtime —all at the organization's expense.

From patching applications and updating firewalls to setting and enforcing administrative privileges, so many elements of the security puzzle can go wrong when handled manually. And as cybercriminals get better at identifying vulnerabilities, relying solely on operations teams to handle these tasks can have detrimental or irrecoverable consequences.

Talent shortages can worsen security gaps

Cybersecurity skills are in short supply, which only increases the likelihood of human error during manual tasks. There are simply not enough people with the skills and training to assess and address security risks. According to the (ISC)^2 Cybersecurity Workforce Study, Australia needs 25,000 more IT security workers to close its cybersecurity gap.[4]

This chronic shortage of cybersecurity experts makes it more difficult for government agencies to adequately manage risk. Their IT teams are already stretched and don't have the time to enforce security processes across the organization—let alone establish them in the first place.

Equipping security teams with automation

Addressing how both manual security processes and skills shortages increase risk for organizations has become essential in the fight against cybercrime, and automation solutions offer a promising solution. As we will explore further, automating security processes provides much-needed consistency, accuracy, and scalability across the organization.

The risk of manual security measures

"Organizations with no security automation experienced breach costs of $6.71 million on average in 2021, versus $2.90 million on average at organizations with fully deployed security automation."[5]

4. "A Resilient Cybersecurity Profession Charts the Path Forward," (ISC)^2 Cybersecurity Workforce Study, 2021.
5. "Cost of a Data Breach Report 2021." IBM, 2021.

03 Common challenges of risk management

Government agencies need better risk management

To ensure the confidentiality, integrity, and availability of official information, government agencies must be able to identify and manage risk, accurately and efficiently. Security threats are constantly evolving, which means an organization's risk profiles and security posture should remain adaptable. Automating operations is critical to be able to rapidly respond to these changes.

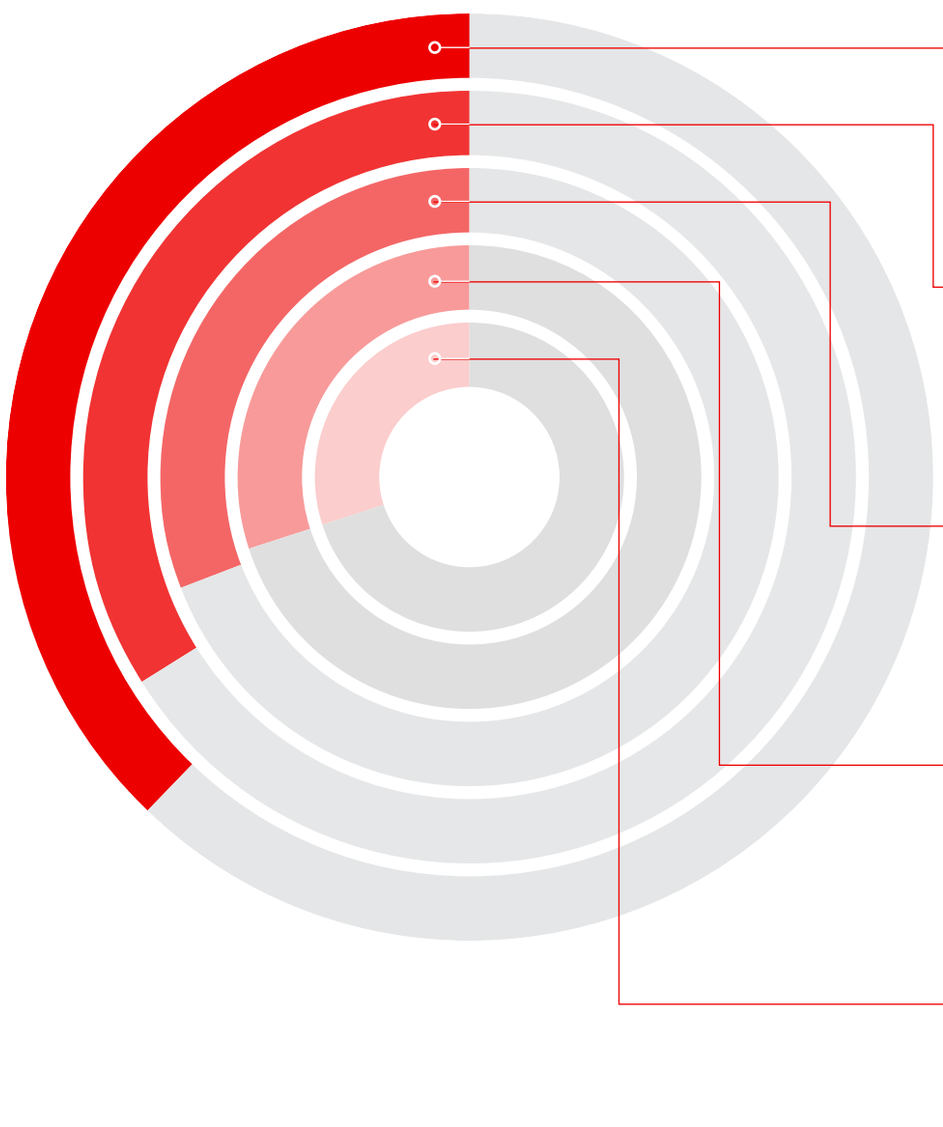
Obstacles to changing security practices

In their effort to enhance security, government agencies face several challenges—particularly related to managing change. Common questions include:

- How do we scale our team to implement a new cybersecurity initiative?
- How do we support different parts of the organization to ensure new security protocols are adhered to?
- What can we do to better secure our existing systems—which deliver critical services—while adopting modern security strategies that the organization needs?
- Can we implement strategies like Zero Trust on established architectures?

However, instead of seeing these considerations as a burden, organizations can view their changing security landscape as an opportunity to reassess their security practice and implement more rigorous protocols.

Common cybersecurity challenges



38%

Keeping up with rapidly changing threats[6]

34%

Educating about risk and behaviour[6]

31%

Shoring up internal cyber security posture[6]

30%

Need for cybersecurity training[6]

30%

Legal/financial ramifications of data breaches[6]

6. "State of the Channel 2021." CompTIA, Aug. 2021.

04 Strengthening your security posture with automation

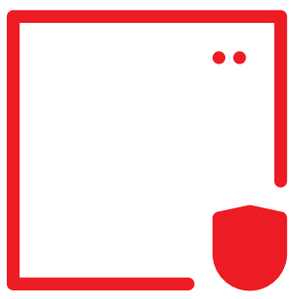
Automating key elements of your cybersecurity strategy

To reduce risk and help combat cybercrime, government agencies are turning to cybersecurity automation. By automating regular, repetitive work, cybersecurity teams can focus on more critical, strategic tasks. Additionally, automation helps avoid overburdening IT teams with tasks and work volume that make human error more likely and increase security risk.

The ACSC Essential Eight explains how automation can be used to bolster your cybersecurity strategy. When implementing the Essential Eight, many organizations struggle with the fact that there is no way to consistently reduce or eliminate human error—especially given current resource constraints and technical skills gaps.

To counter this problem, IT leaders are realizing that some elements of their security framework can and should be automated. These examples explain how and where it makes sense to adopt automation in your organization:

Automating the ACSC Essential Eight

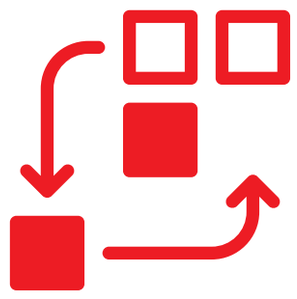


Application control

Automated changes to application control state across the hybrid cloud

Application and operating system patching

Automated preflight checks, content promotion, and post-update verification and testing



Backup and restore

Automated backup, restore, and verification testing

Refining the process of patching

To help prevent attacks, the Essential Eight recommends that organizations regularly patch applications and regularly apply updates to protect against malicious security issues. Patching applications as soon as updates are available is not only best practice, but often, it's also a regulatory requirement. That said, manual patching is always vulnerable to human error, and it can be particularly time consuming in large organizations.

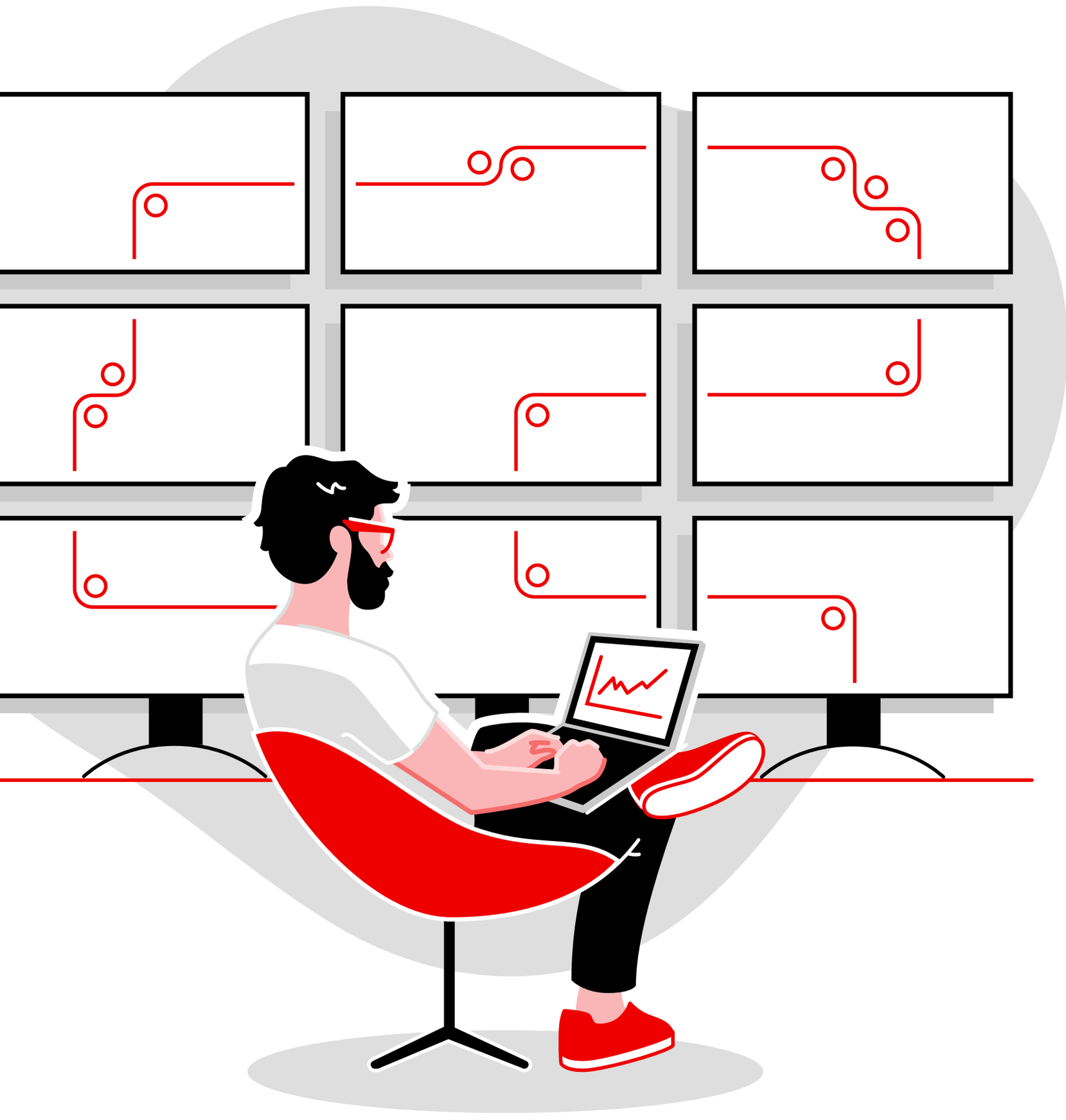
Patching is a great use case for automated workflows. Instead of relying on an IT employee to perform testing, set up preflight checks, and run the patches, organizations can automate verification and testing. Doing so ensures all these steps proceed smoothly and efficiently, with the proper security in place behind the scenes.

Managing administrative privileges

To limit the extent of attacks, the Essential Eight recommends that organizations restrict administrative privileges. Controlling privileged access helps provide security for infrastructure and applications, run business processes efficiently, and maintain the confidentiality of sensitive data and critical infrastructure.

Only a small handful of people within your organization should have global control. Determining who should have privileges can be difficult. Estimating the blast radius of a security incident—and evaluating the total impact of that potential event can be challenging as well, but this practice allows you to anticipate what will happen if someone does misuse their credentials. Then, your IT team can implement security measures to ensure such an incident doesn't affect the whole organization.

By automating privileged access management workflows and storing access credentials centrally—without having to inject these into applications where they can potentially be leaked—the whole process becomes much more manageable and reliable.



05 Red Hat's role in your cybersecurity approach

Building a future-ready cybersecurity practice

Red Hat® solutions can help you automate your existing manual processes, allowing you to mitigate the risk of oversights due to overburdened, understaffed IT teams in your organization. Our open source products deliver flexibility and scalability across cloud environments and architectures, which supports organizations as they deploy in their current and future environments.

Using automation at the foundation of any cybersecurity maturity model, any organization can take practical steps to quickly and iteratively add layers of automation and replace manual processes. And Red Hat solutions can help with both risk mitigation and response.

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform is built with Ansible, a human-readable automation language that takes complex manual processes and turns them into automated workflows. Ansible Automation Platform allows your IT teams to automate and integrate different security protocols across the enterprise. Using this platform, your organization can investigate and respond to threats in a coordinated, unified way using a curated collection of modules, roles, and playbooks.

Red Hat Ansible Automation Platform allows organizations to automate:

- Patching for common vulnerabilities and exposures (CVEs).
- Application control rollout.
- Backup and restore or verification processes.

Ansible Automation Platform provides a security-focused, stable enterprise framework for building and operating IT automation at scale, from hybrid cloud to edge environments. This automation solution allows users across an organization to create, share, and manage Ansible Playbooks from developer and operations teams to security and network teams. IT managers can provide guidelines on how automation is applied to individual teams, and automation creators can write tasks that use existing knowledge.

Additionally, Ansible Automation Platform can serve as an integration point for security solutions as it contains content from certified partners like CyberArk, IBM, and Splunk, which can be used to automate the management and integration of security technologies.

Learn more about Ansible Automation Platform ›

Red Hat Enterprise Linux

Red Hat Enterprise Linux® provides a foundation for scaling existing applications and rolling out emerging technologies across bare metal, virtual, cloud, and edge footprints with consistent security.

Red Hat Enterprise Linux takes a practical, three-point approach to addressing security challenges:

- Mitigate: Manage security and reduce the risk of a breach before your data, systems, or reputation are exposed.
- Protect: Automate security controls and maintain them over time, at scale, and with minimal downtime.
- Comply: Streamline compliance standards for organizations with highly regulated environments.

Red Hat Enterprise Linux also contains built-in security policies aligned with ACSC guidance, like the Information Security Manual (ISM) and the Essential Eight, to help government organizations better manage risk by automating the rollout of security controls to new digital services, simply and consistently.

Learn more about Red Hat Enterprise Linux ›

Red Hat

Previous

Strengthen your security with Red Hat

Red Hat is here to help improve the security of your digital services

Red Hat can help you automate guidance from the ACSC and better manage risk with automated security integrations.

To learn more, get in touch today >