Cyber Secure

Module 6

Neglecting Software Updates

Author: George Nicholl

Student ID: 50095130

Keeping software up to date is one of the simplest yet most essential defences against cyber threats. Software vendors routinely release updates to fix bugs, patch security vulnerabilities, and improve functionality. However, many users and organisations delay or ignore these updates, leaving systems exposed to known and easily exploitable threats.

This module compliments the training video by expanding on the technical risks, real-word consequences and best practices for maintaining up-to-date systems.

What is the Risk of Neglecting Software Updates?

Every day that a known vulnerability remains unpatched increases the chance of it being exploited. Neglecting software updates means failing to install patches that fix known vulnerabilities. Every day that a system remains unpatched increases the chance of it being exploited. Attackers actively scan the internet for unpatched systems and use automated tools to exploit them at scale. These attacks can lead to data breaches, ransomware infections, and system takeovers - all from vulnerabilities that already had fixes available.

In 2024, attacks targeting known vulnerabilities increased by 54% (Security Boulevard, 2024). This shows a clear preference by attackers for exploiting unpatched software over complex zero-day exploits.

- **Increased Risk of Exploitation**
  In 2024, attacks on known vulnerabilities increased by 54%, as attackers increasingly focused on low-effort, high-reward targets rather than sophisticated zero-day exploits (Security Boulevard, 2024).
- **Ransomware Delivery Method**
  According to Sophos (2024), 32% of ransomware attacks in the past year originated from unpatched software vulnerabilities. This means a third of ransomware infections could have been prevented simply by applying available updates.
- **The True Cost of Ignoring Patches**
  BankInfoSecurity (2024) reported that 60% of cyber compromises in 2024 were due to unpatched vulnerabilities. This includes breaches of major corporations, government entities, and small businesses alike.
- **Financial Repercussions**
  SecureFrame (2024) found that the average cost of a data breach rose to $4.88 million, with outdated software listed as one of the top contributing factors. The cost includes investigation, remediation, legal fees, regulatory penalties, and reputational damage.

Common Threats or Mistakes

A. **Delayed Patch Deployment**

- Postponing updates for convenience or due to resource complaints
- Critical patches may go uninstalled for weeks or months

B. **Misconfigured Update Settings**

- Automatic updates turned off or misconfigured
- Systems never receive essential security patches

C. **Ignoring Third-Party Applications**

- Focus on only Operating System updates while neglecting browsers, plugins or productivity apps
- Third-Party software is often targeted as a backdoor

D. **Lack of Visibility and Ownership**

- No clear assignment of patch responsibilities within IT or security teams
- Leads to missed updates and uncoordinated patching efforts

These issues are especially prevalent in organisations without a formal patch management policy.

Real World Examples

- In 2017, the WannaCry ransomware attack affected over 200,000 computers across 150 countries. The exploit targeted a known vulnerability in Microsoft Windows - one that had already been patched months earlier. Organisations that had delayed updates were severely impacted.
- In 2023, a major U.S. health provider suffered a breach when attackers exploited an unpatched vulnerability in a third-party application. The breach affected millions of patient records and resulted in heavy regulatory fines.

Consequences of Neglecting Updates

- Security Vulnerabilities – Open paths for attackers to exploit
- Downtime and Disruption – System failures, ransomware and outages cause operational chaos
- Compliance Violations – Breaching regulations like GDPR or HIPAA due to preventable security lapses.

- Financial Loss – The average data breach now costs $4.8 million (SecureFrame, 2024)

Best Practices for Patch Management

A. Establish a Patch Management Policy

- Define roles responsibilities, and patch cycles
- Prioritise critical updates and track implementation

B. Use Automated Tools

- Employ update management software to apply patches quickly
- Reduce reliance on manual intervention

C. Monitor Vendor Alerts and Bulletins

- Stay informed about newly disclosed vulnerabilities
- React swiftly to high-risk updates

D. Test Before Full Deployment

- Use a staging environment to prevent compatibility issues
- Apply updates across production systems after verification

E. Include All Software Types

- Cover Operating Systems, applications, plugins, SaaS, and mobile platforms

F. Educate End Users

- Promote awareness of update prompts
- Encourage prompt installation on all devices

Key Takeaway

Neglecting software updates is like leaving your front door open in a high-crime neighbourhood. Most cyberattacks do not require advanced hacking skills – they exploit known issues with available fixes. In a world where cyber threats evolve rapidly, staying current with patches is one of the most cost-effective and powerful ways to protect digital assets. By making software updates a non-negotiable part of your cybersecurity strategy, you significantly reduce the chances of falling victim to preventable attacks.

Why This Matters for You

Whether you are a developer, admin or end user, staying on top of software updates is essential. Timely patching helps prevent breaches, reduce downtime and maintain trust across your organisation.

Quick Recap: Software Update Best Practices

DO:

- ✔ Enable automatic updates wherever possible
- ✔ Prioritise critical security patches and apply them promptly
- ✔ Monitor update alerts from all software vendors
- ✔ Include browsers, plugins, and SaaS tools in patching plans
- ✔ Test updates in staging before full rollout (for enterprise)

DON'T

- X Don't assume updates are handled automatically without confirmation
- X Don't ignore update prompts or postpone installations
- X Don't limit patching to just the operating system

References

BankInfoSecurity (2024) *Unpatched Vulnerabilities Cause 60% of Cyber Compromises*. Available at: https://www.bankinfosecurity.com/unpatched-vulnerabilities-cause-60-cyber-compromises-a-26051 (Accessed: 2 April 2025).

Security Boulevard (2024) *Impact of Unpatched Vulnerabilities in 2025*. Available at: https://securityboulevard.com/2024/12/impact-of-unpatched-vulnerabilities-in-2025 (Accessed: 2 April 2025).

Sophos (2024) *The State of Ransomware 2024*. Available at: https://www.sophos.com/en-us/content/state-of-ransomware (Accessed: 2 April 2025).

Secureframe (2024) *Data Breach Statistics 2024*. Available at: https://secureframe.com/blog/data-breach-statistics (Accessed: 2 April 2025).

Microsoft (2017) *WannaCry Ransomware Attack Analysis*. Available at: https://www.microsoft.com/security/blog/2017/05/12/wannacry-ransomware-attack-analysis/ (Accessed: 2 April 2025).