2017 SECURITY PATCHING IS HARD

Survey results

0PATCH

Overview

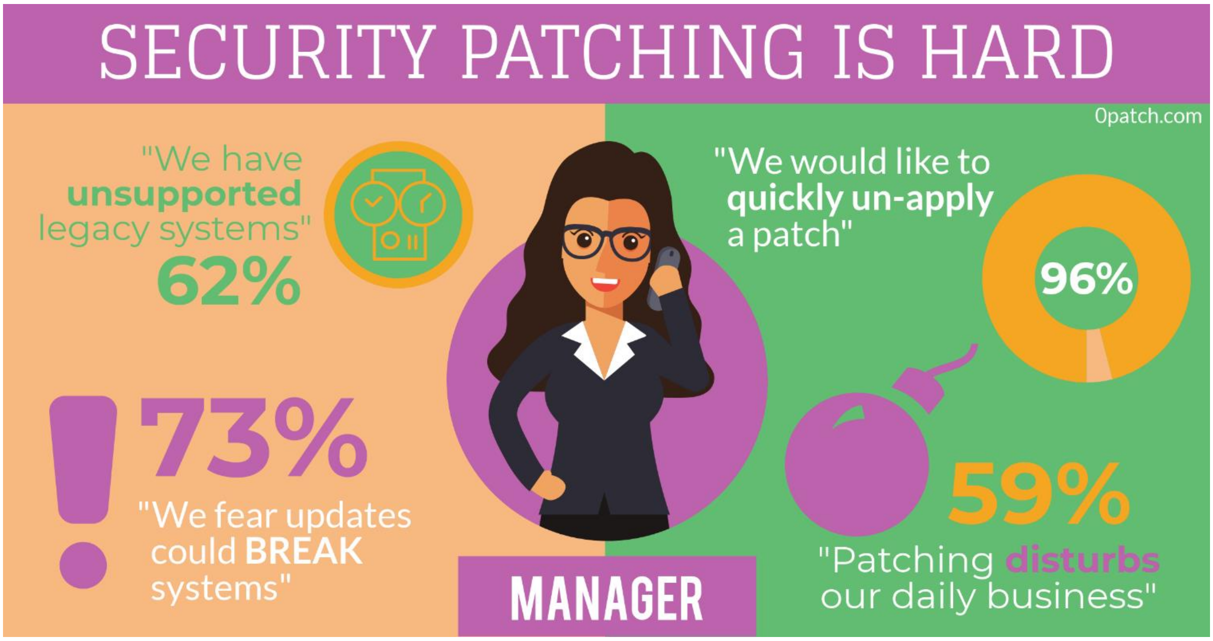
Applying software patches and updates seems to be a crucial task if we want to keep our computers secure. Timely software patching may be a requirement of many authoritative standards and regulations. The „common sense“ dictates that one should not delay applying security patches. And as usually, the reality turns out to be much more complex.

This is our first survey revealing struggles and obstacles companies and individuals deal with when they try to be up to date with security patching. It was inspired by security-aware individuals that opened the debate of their patch fatigue after the Equifax attack. One thing to keep in mind is that our respondents reach was somewhat limited to social media bubbles and our geographical location, but we truly hope to make it an extended and repeatable exercise over the following years.

So why is patching such a challenge to execute? Before we dive into a detailed exploration of existing security gap, let‘s reveal our respondents‘ top answer:

It is hard because it could break systems.

CONTENTS



SECURITY PATCHING IS HARD
0patch.com
"We have unsupported legacy systems"
62%
"We would like to quickly un-apply a patch"
96%
73%
"We fear updates could BREAK systems"
MANAGER
59%
"Patching disturbs our daily business"

KEY TAKEAWAYS

72%

"Security patching is hard because it COULD BREAK STUFF."

Administrators, managers and security experts agree: it's NOT inadequate money or staffing.

58%

"WE HAVE **LEGACY** SYSTEMS working on UNSUPPORTED PLATFORMS that would be EXPENSIVE to update or replace."

"Being able to **quickly un-apply** a patch

88%

would help us sooth our patch fatigue."

79% **Decoupling** security patches from the functional ones would help accelerate applying security patches.

53%

"We experience **incompatibilities** with our applications and latest OS version."

Managers:

"We **don't want**

52%

functionality changes

that come with security patching."

By the Numbers PEOPLE

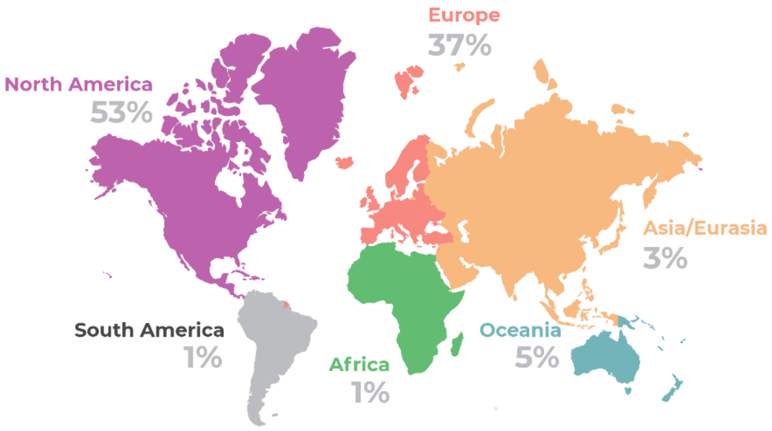
„Security Patching is Hard 2017“ survey was conducted from the beginning of June to the end of August 2017. We received 340 answers, majority of them from North America and Europe. Answers came from 38 countries: 156 from United States, 26 from UK with Northern Ireland and Slovenia (yes, that‘s where we come from), 16 from Canada, 15 from Germany.

For the sake of simplicity we classified industries in 26 categories, 6 of which represent 72% of respondents, with „Technology“ as the prevailing answer.

We assumed different job roles would provide job-specific answers. „IT Administrators“ and „IT Security Specialists“ were in majority, followed by „Managers/C-level Managers“.

We did not ask specific questions about their patch management processes or the tools they are using.

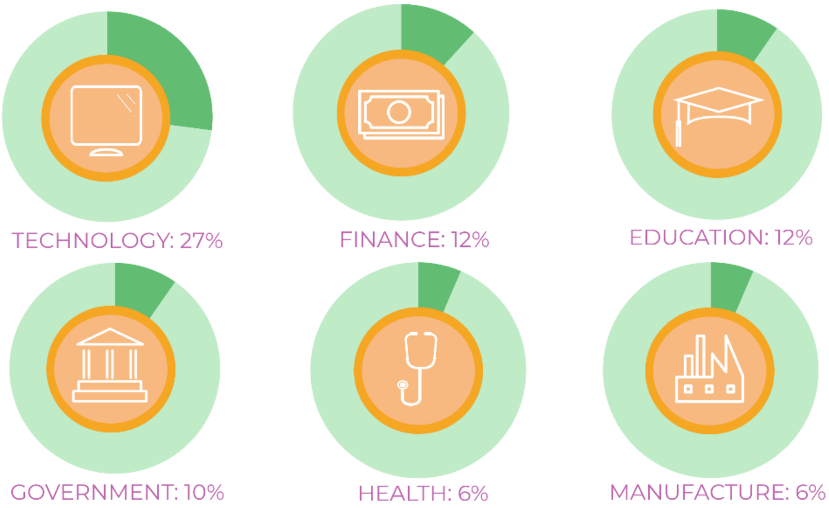
COUNTRIES



Q1: In what country do you work?

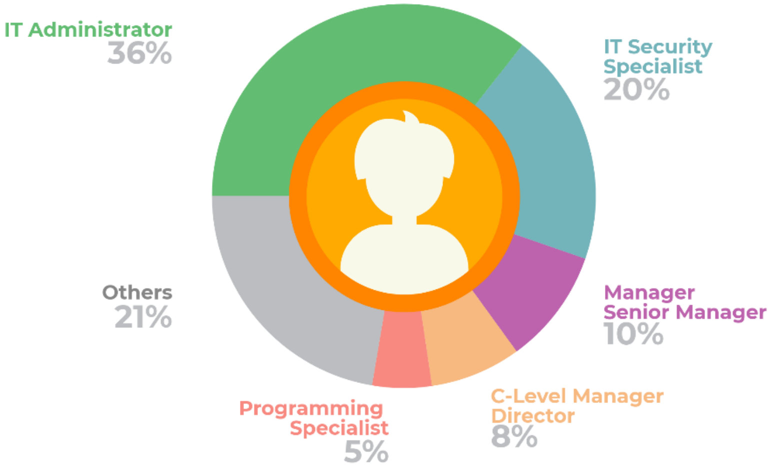
By the Numbers PEOPLE

INDUSTRIES



Q2: Which of the following best describes the principal industry of your organization?

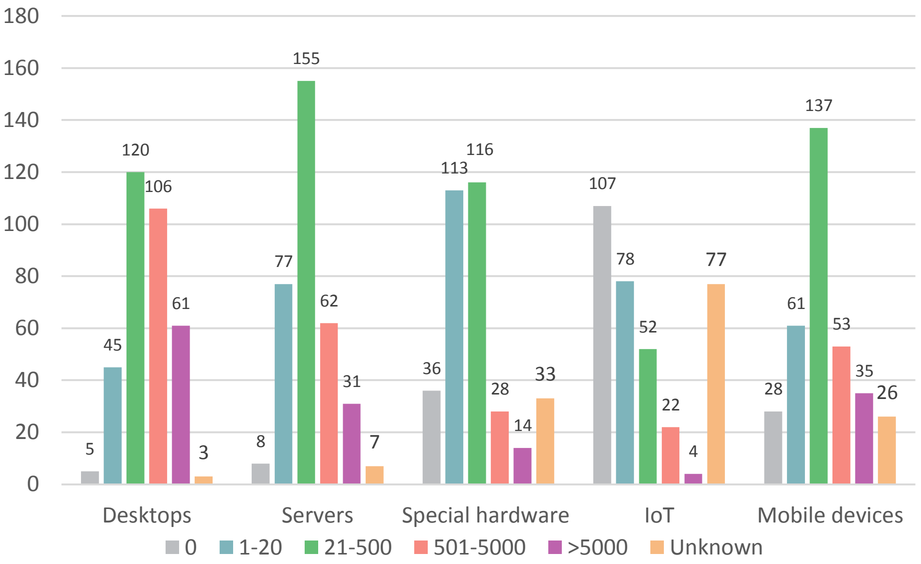
JOB ROLES



Q3: Which of the following describes your job role best?

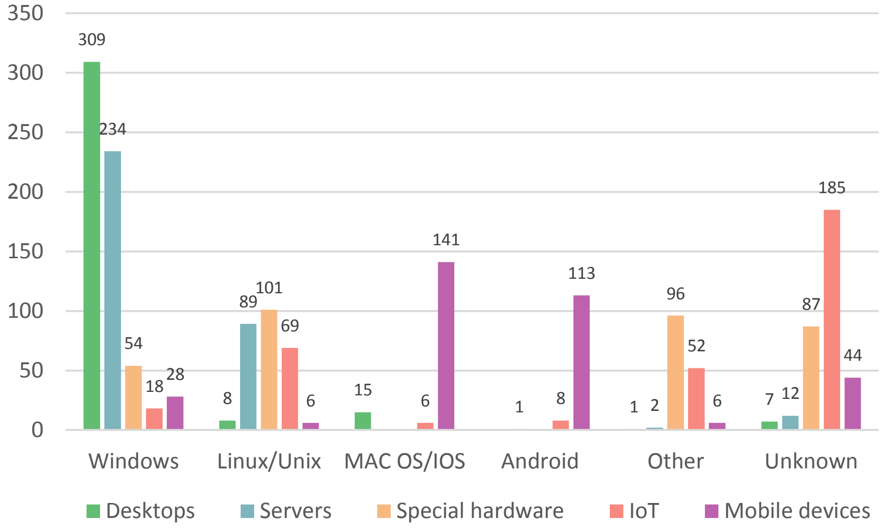
By the Numbers DEVICES

The survey answerers are operating in small, big and huge networks. Prevailing participants‘ networks consist of 21-500 desktops, servers, special hardware and mobile devices.



Q4: How many computer systems are in your network?

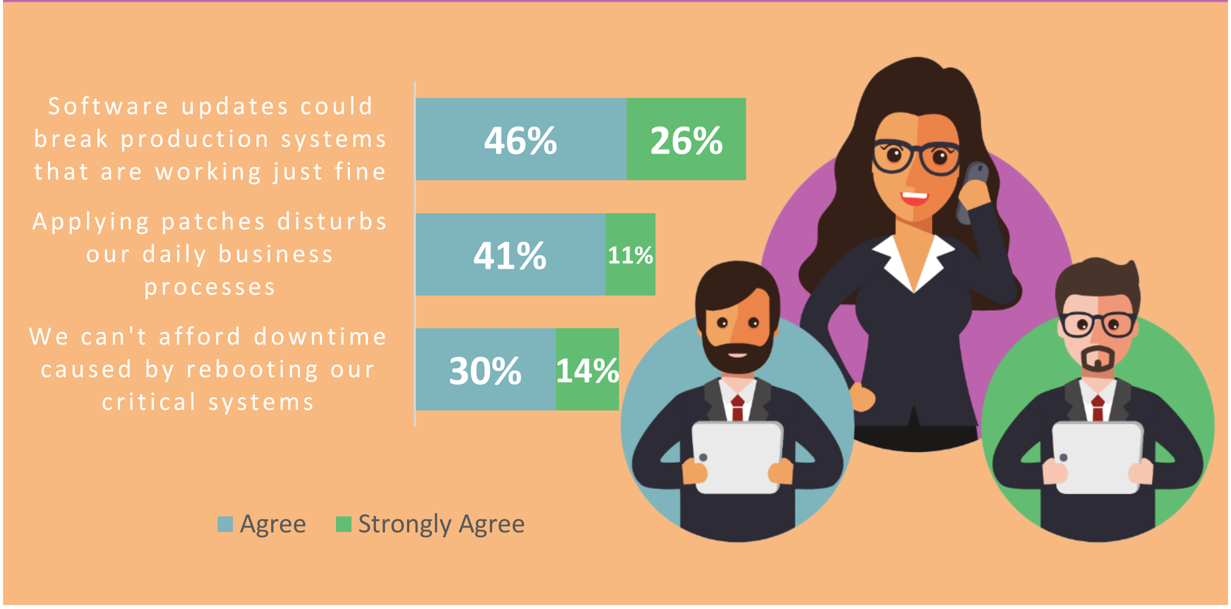
Our respondents‘ hardware inventory on servers and desktops is still dominated by Windows. There are obvious unknowns about operating systems running on special hardware and IoT devices and this could present future security risks.



Q5: Which is the prevailing operating system in your network?

Security Gap MAIN REASONS

TOP 3 REASONS FOR SECURITY UPDATE GAP



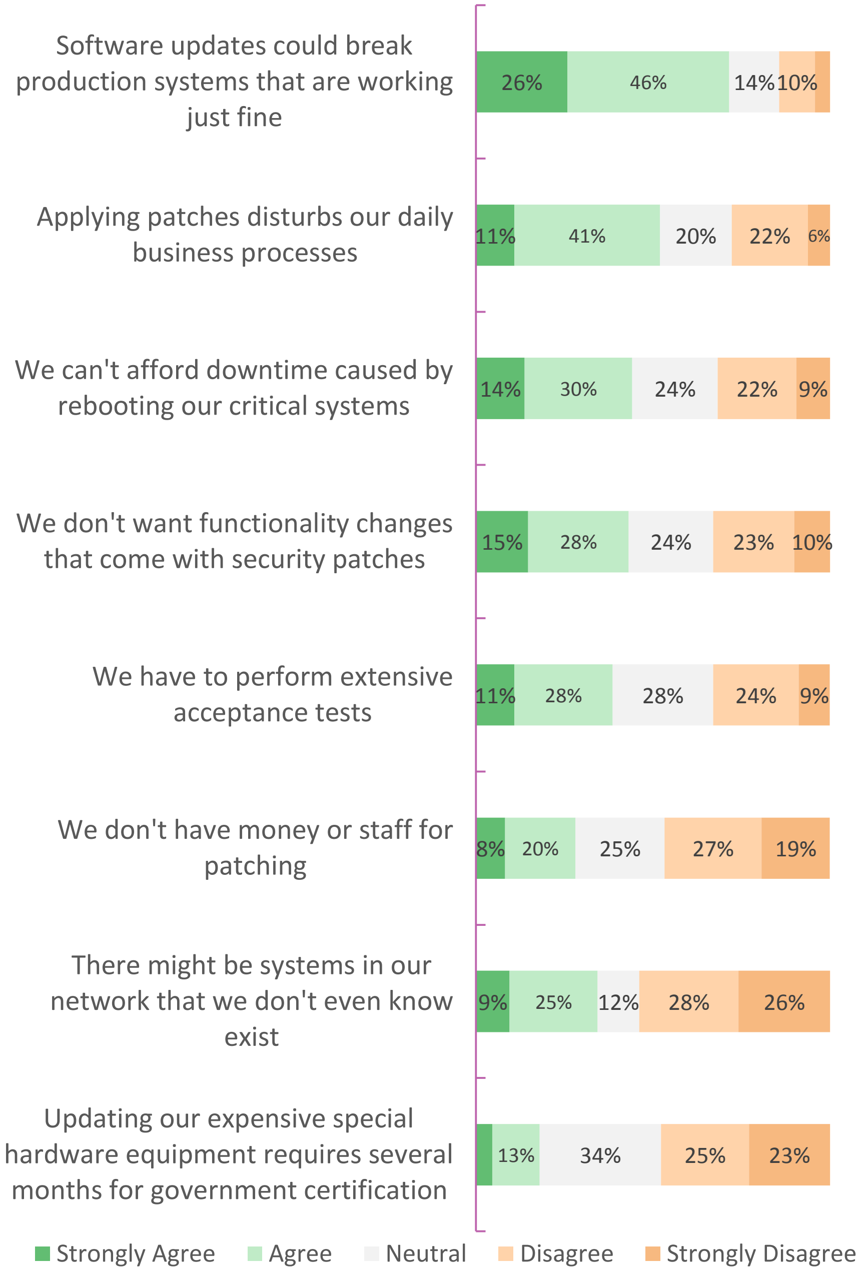
Staying up to date with software versions in a complex enterprise or even home IT environment could be overwhelming, but neglecting security patches that are often released at an unmanageable rate could lead to poor cybersecurity hygiene.

There‘s not just one simple reason for the wide security gap in many enterprise networks, but according to our survey results IT administrators, security professionals and managers strongly agree that the main reasons are not related to lack of money or security awareness.

Almost three quarters of respondents worry that software updates could break their production systems. **More than half** of them don‘t want to be disturbed during their business processes. **Almost half** of IT personnel can‘t afford downtime caused by rebooting critical systems and dislike functionality changes rolling out with security patches.

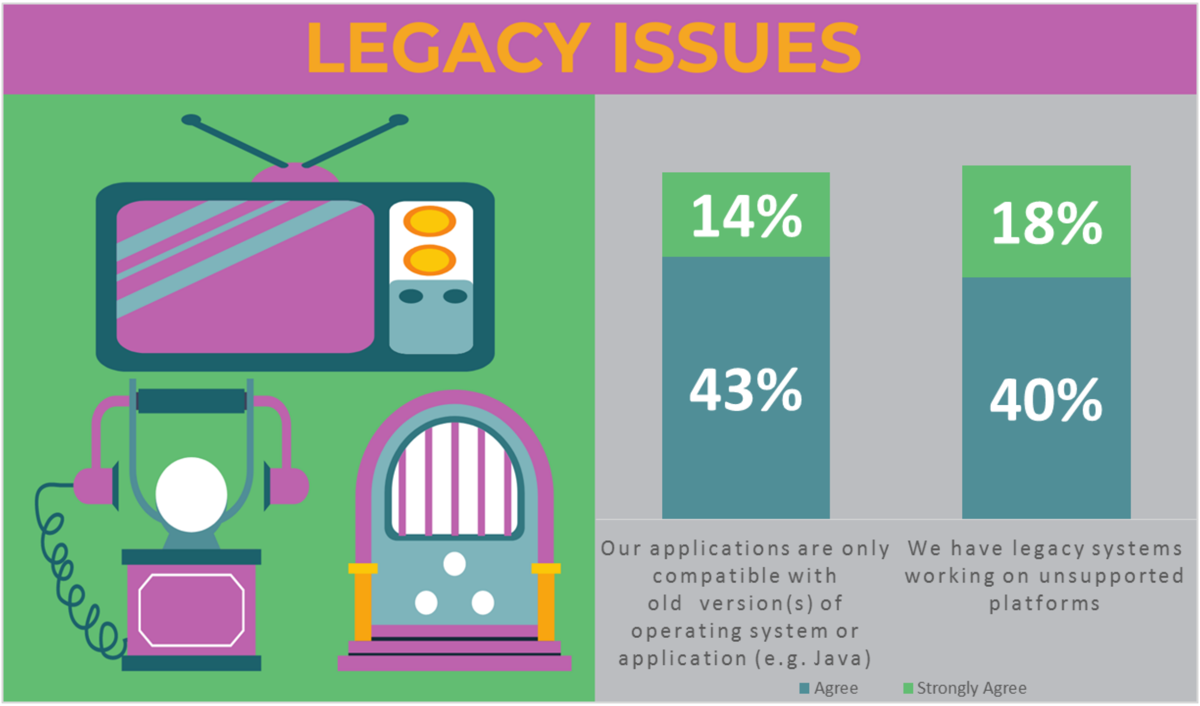
In the segment of **enterprises with high volume** (>500) of special equipment, 73% respondents complain that they have to perform extensive acceptance tests.

Security Gap



Q6: Main Reasons for the Security Update Gap

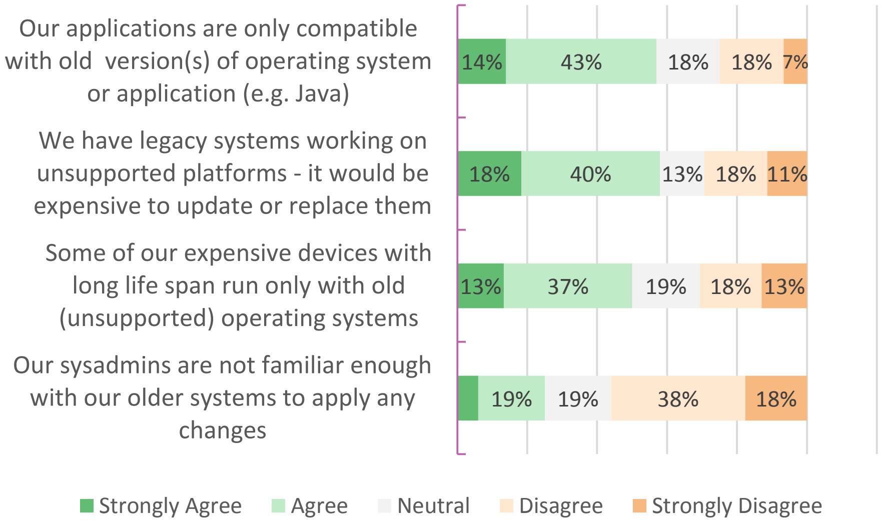
Legacy Issues



It‘s hard to combine old and new worlds, but it‘s also a challenge to replace antiques with novelties. **Special expensive devices** (such as medical equipment or industrial machines) are expected to live for decades, but their embedded core operating system‘s working life expectancy is much shorter – usually five to ten years. With Windows 10 semi-annual feature updates this period is getting even shorter.

Banking, travel, public sector and other traditional industries are conservative in changing stable platforms and well tested processes. It just has to make business sense to replace a key software framework with a newer version. Due to possible incompatibilities between installed applications the respondents are reluctant to upgrade one or all of them in order to avoid future inconsistencies. So why fix it if it isn‘t broken?

Legacy Issues



Q7: Security patching is hard because of legacy issues

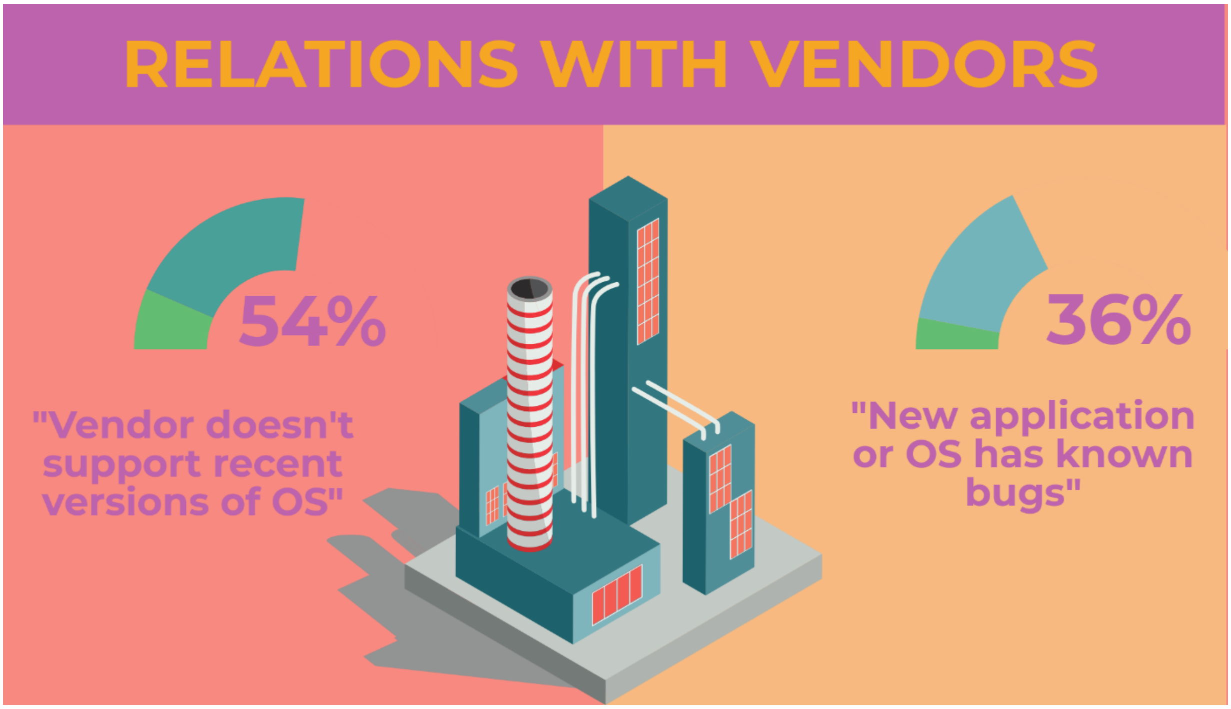
A strong majority of respondents experience incompatibilities between their applications (e.g. Java) and latest OS versions. They are also dependent on legacy systems working on unsupported platforms that are expensive to update or replace.

Half of them struggle with patching of their expensive devices with long life span that run on old or unsupported operating systems.

It sounds alarming, but **a quarter** of participants believe their limited understanding of older computer systems makes them afraid to apply any changes to them.

In addition to answering survey questions **respondents commented** that they have hard time patching legacy software because of bad architectural or design decisions made in the past. They also said that they don‘t have adequate validation and smoke tests for critical applications and that patching results are not verified by stakeholders.

Relations with Vendors



Q8: Security patching is hard because of relationship with vendors

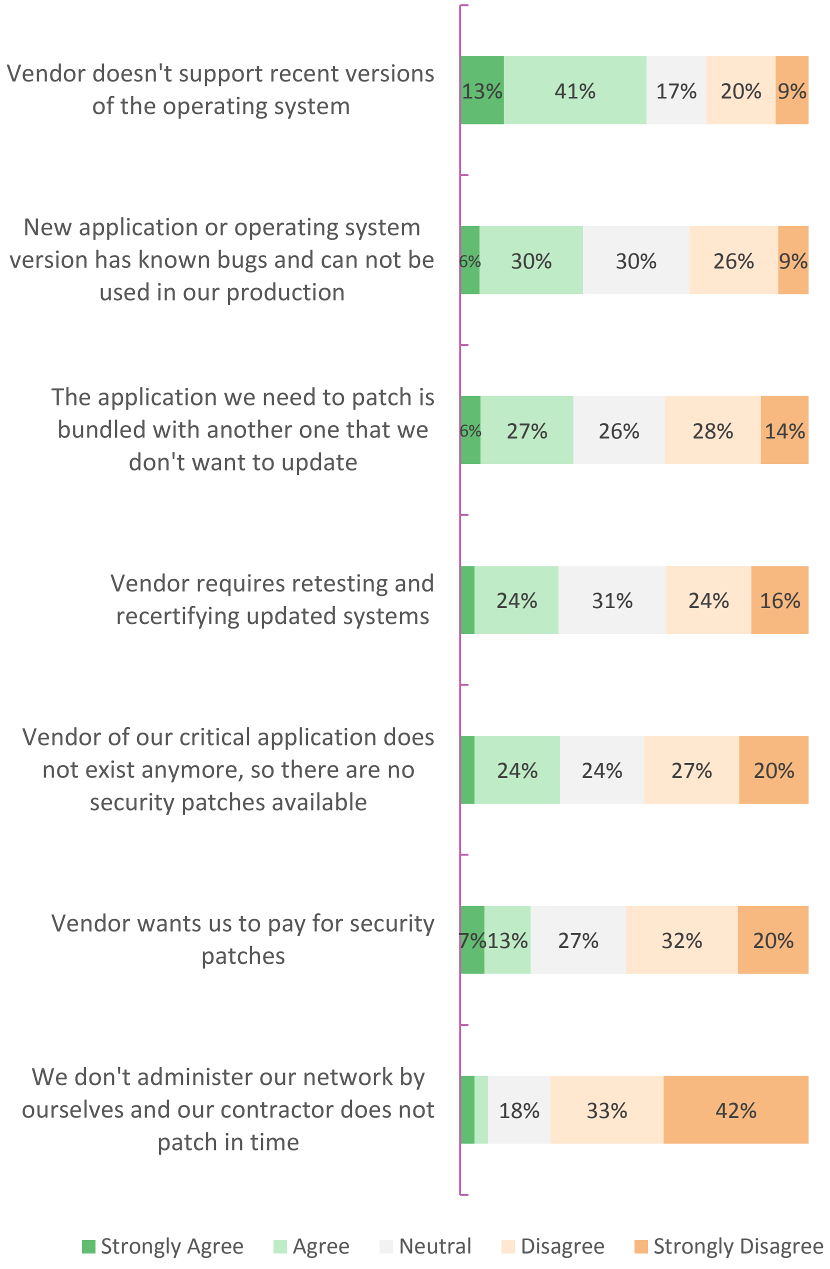
In the context of software patching the relationship between computer users and software vendors is summarized in a key question: is it possible to run the application on the latest OS version?

More than a third of survey participants expect new software to introduce security bugs or can't apply an existing patch because it is bundled with software they are not able to update. For **a quarter or more** of participants patches are not available because the vendor does not exist anymore. A similar percentage agrees that applying patches would require extensive testing and recertifying.

Large enterprises (>5000 desktops, >500 special devices) suffer from retesting and recertifying of updated systems. **20% of respondents** answered that they had been asked by vendors to pay for security patches.

In addition to answering survey questions **respondents commented** that if they are not on the most current build, patching an older version can sometimes be problematic. Patching could also be dangerous due to insufficient support by the software vendor.

Relations with Vendors



Q8: Security patching is hard because of relationship with vendors

The Need for Change

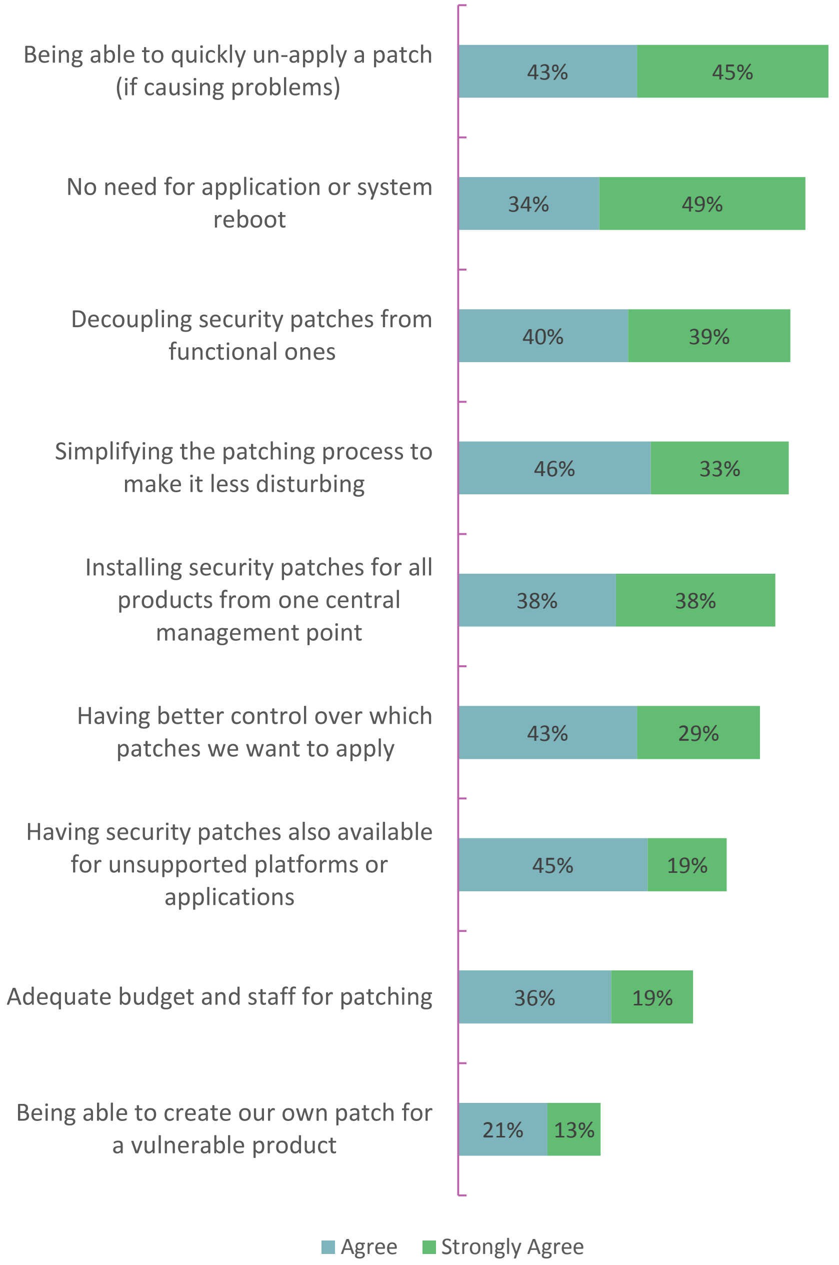
If there is one clear message out of this survey it would be: if we want to narrow the security update gap and relieve the existing patch fatigue **the process of patching should be much simpler**.

So what are the next steps to make software patching at least bearable, if not painless, easy and effortless? **88%** suggest that they should be able to quickly un-apply a patch. **83%** of answerers are disturbed by mandatory restarting of applications or systems and **79%** would appreciate security patches being decoupled from functionality changes.

Three-fourths would appreciate having better control over all patches they apply, preferably installing them from one central management point.

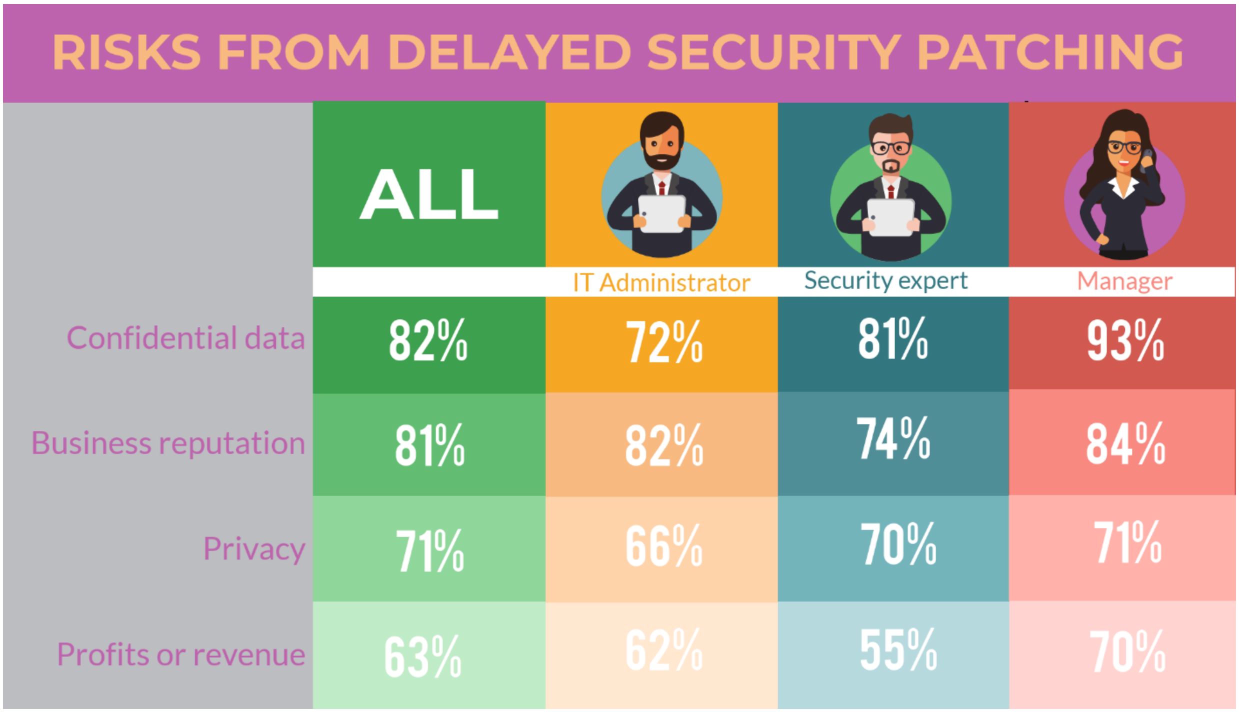
In addition to answering survey questions **respondents commented**: mobile devices are often out of network, equipment is switched off and all this can delay patch deployment. They prefer just the change of code bits, not entire libraries. They appreciate having complete and frank information on the patch from software vendor („if it adds telemetry don‘t call it a fix“, said one of them). Participants also expressed the need for better vendor support for security patching.

The Need for Change



Q9: What changes in your patching process would help you accelerate applying security patches?

Risks from Delayed Security Patching



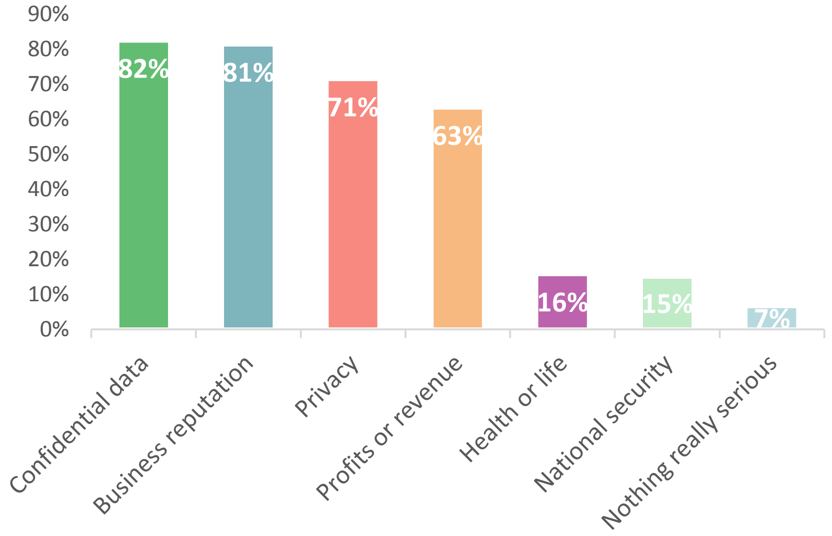
RISKS FROM DELAYED SECURITY PATCHING

	ALL	IT Administrator	Security expert	Manager
Confidential data	82%	72%	81%	93%
Business reputation	81%	82%	74%	84%
Privacy	71%	66%	70%	71%
Profits or revenue	63%	62%	55%	70%

There‘s a significant difference in assessing risks from delayed security patching among various security stakeholders in organizations. Having responsibility for compliance with latest privacy legislation and bouncing everyday attack attempts, managers express higher risk concerns due to delayed security patching in all top categories.

On the other hand, just over half of security experts perceive delayed security patching as negatively impacting profits or revenue of their company.

Risks from Delayed Security Patching



Q10: What are the Risks from Delayed Security Patching? (multiple choice question)

Only 7% of respondents perceive risks from delayed security patching as a non-issue. For **more than 80%** delaying security patching is causing a risk of confidential data or business reputation loss.

FINAL THOUGHTS

Security patching is really hard.

Timely security patching plays an important role in providing a secure enterprise IT environment, but dealing with patches as they are released at an unmanageable rate seems to be an overwhelming task.

Individuals responsible for patching are facing several difficulties and are suffering from patch fatigue that is tough to remediate. Security patching is hard because it could break stuff or disturb daily business. Enterprises can‘t afford downtime caused by rebooting of their critical systems. IT experts hate functionality changes that come with patches and don‘t want to lose time performing extensive acceptance tests.

Some applications or expensive devices are only compatible with old versions of software or their legacy systems are working only on unsupported operating systems. New versions of applications or operating systems have known bugs and can‘t be used in production or are bundled with other software that they don‘t want to update.

So what is the recipe for eliminating the existing security update gap? **There‘s clearly a need for change.**

Experts should be able to quickly switch off patches if they are causing problems. There should be no need for application or system rebooting. Security patching should be decoupled from functional changes. There should be better control over patch management, preferable from one central management point.

The process of patching should be simplified.

Contact Us

0patch.com
@0patch

PATCH

0patch by ACROS Security (0patch.com) is a pioneer in re-inventing software patching. 0patch is a platform for instantly distributing, applying and removing microscopic binary patches to/from running processes without having to restart these processes (much less reboot the entire computer).

ACROS Security (www.acrossecurity.com) is a leading provider of security research, realistic penetration testing and code review for customers with highest security requirements.