Getting Your House in Order

Why businesses are leaving doors open to security breaches and what must be done to close them

Foreword

Sumir Karayi, CEO, 1E

Given the severe damage caused by the NotPetya and WannaCry attacks, which impacted many businesses for months, we recently felt compelled to sponsor a large research project to determine whether the situation had improved since those devastating attacks swept through the world.

Hence this report. 1E commissioned respected research house Vanson Bourne to survey 600 senior IT decision-makers (300 from IT Operations and 300 from IT Security) across the US and UK, to get a proper picture of the cybersecurity challenge from both sides of the IT fence.

Security built on sand

Like me, you may think the findings are both interesting and disturbing. 60% of organizations told us that they have suffered a serious cyber breach in the last two years. Over 30% have suffered more than one.

Yet the situation is still not under control. These events are avoidable but unless something changes soon, our data suggests we will have to brace ourselves for more major breaches in the near future.

This report highlights the causes for this, such as a lack of visibility and control across one third of endpoints, a crisis of trust between IT Security and IT Operations, and the ongoing struggle to patch software or even keep Operating Systems current.

New challenges such as the digital revolution and mobile workforce are only making the problem worse.

However, our report shows that the situation, although serious, is by no means beyond repair.

We have asked several experts for their guidance and opinion on how to improve this situation and we welcomed input from Shira Rubinoff (President and Co-founder, Prime Tech Partners), Kurt De Ruwe (CIO of Signify – formerly Philips Lighting), Jason Sandys (Microsoft MVP), Jason Keogh (ISO standard SC7/SC27 liaison) and Talal Rajab (Cyber Security Head, Tech UK).

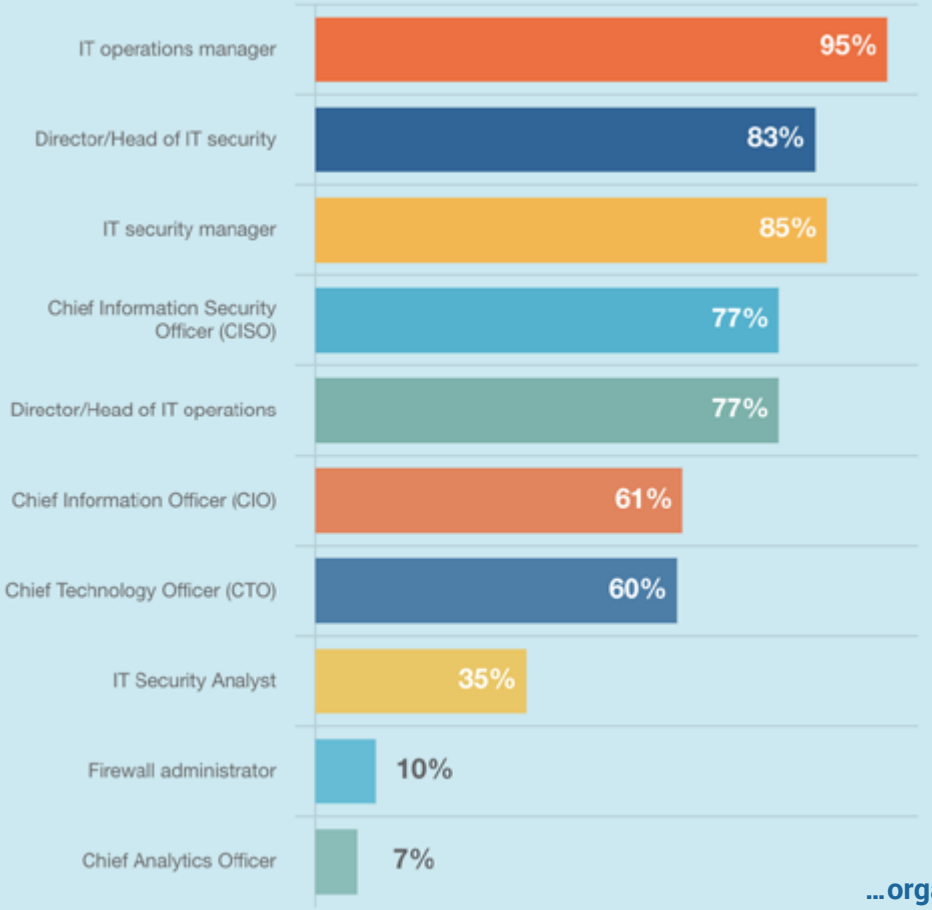
We also asked one of the leading security experts in the world, Michael Daniel, former cybersecurity advisor to President Obama, and currently President & CEO of the Cyber Threat Alliance, to develop a 10-Point Action Plan based on the data.

I hope you enjoy reading this report as much as we enjoyed researching it. The study points to a big opportunity for every organization to become much more secure.

Respondent Information

300 operational IT decision makers, and 300 security IT decision makers were interviewed in February and March 2019, split in the following ways…

…respondent job role



"Which of the following most accurately describes your position in the organization?" asked to all respondents, showing operational roles in green and security roles in pink (600)

…organization size

"How many employees does your organization have in your country?" asked to all respondents (600)

Source: 1E survey of 600 UK & US IT decision makers, Feb/March 2019

The scale of the problem

Not as safe as houses

“Why are companies vulnerable? Because they run older versions of operating systems, and older versions of software, without patching, and without proper encryption where it’s needed.”

Kurt De Ruwe

CIO of Signify (formerly Philips Lighting)

IT today is a fraught and overstretched environment: 93% of respondents tell us they are experiencing challenges. Amongst a wide range of issues, the leading ones are restrictive budgets, a lack of understanding between IT Operations and IT Security, and legacy systems.

It's possible to trace the connection between these root problems and the prevalent uncertainty felt around the issue of cybersecurity; less than a quarter (23%) believe that they are extremely well prepared to react to a serious data breach.

The anxiety is well founded. 60% of respondents have experienced a serious security breach in the last two years – 31% more than once.

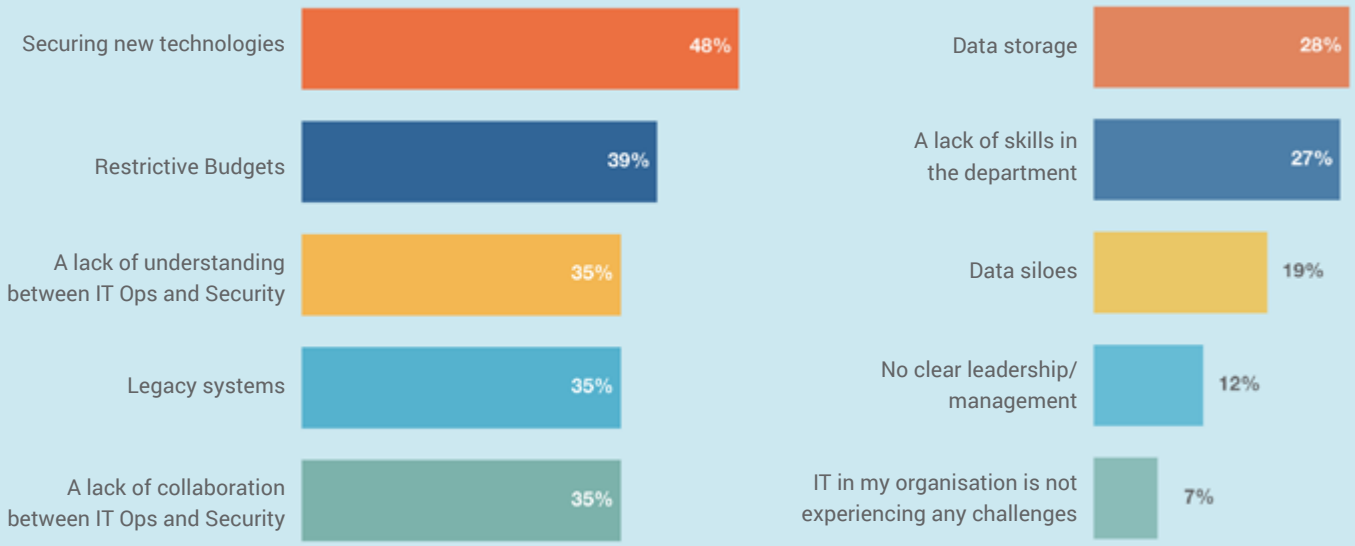
Respondents identified a lack of clear security protocols (52%) and unpatched software (51%) as the principal causes of breaches, followed by a lack of IT Security/ Operations collaboration (42%) and a lack of patch automation (40%). It's easy to see how an organization's cultural issues and technical shortcomings can enforce one another, creating heightened vulnerability.

The concern is that it typically requires a serious wake-up call for the wider organization to act. Even then, the usual knee-jerk reaction is to buy yet another new security tool, rather than address the underlying issues. In other words, they choose to buy another fancy alarm system rather than shutting those windows and doors.

"Too often I see organizations expend far too much budget and resources on new and expensive tools. But the real problem isn't always down to a lack of technology – it's often the lack of a cohesive relationship between IT Security and IT Operations, which can result in gaping holes in the organization's security profile."

Michael Daniel
Former Special Assistant to President Obama and Cybersecurity Coordinator at the White House

Challenges facing the IT department



Which of the following challenges do you believe the IT department, as a whole (including IT Operations, IT security etc.), is currently experiencing in your organisation?" asked to all respondents, showing a combination of responses ranked as the first, second, and third biggest challenge (600)

Source: 1E survey of 600 UK & US IT decision makers, Feb/March 2019

New ways of working

Digital transformation is a mixed blessing to our respondents, with 80% claiming that it increases cyber risk.

Dependence on software is also increasing – a clear majority (73%) told us they were more dependent on it now than they were 12 months ago.

The Dark Web has made it easier for attackers to monetize stolen data. As the value of data has increased, so has the funding and sophistication of the cyber-criminals seeking to exploit vulnerabilities in software. Breaches are becoming more frequent and more damaging.

The growth of remote working is a further key feature of digital workplaces that respondents have flagged as problematic. In fact, until organizations can find a way to effectively reach, patch, and secure those outside the office, remote working will remain a security concern for over three quarters (77%) of respondents.

This is an extremely telling figure. By and large, IT remains dependent on legacy systems developed for the office-based, LAN-style workplace of the 1990s. How can they hope to adequately patch and manage the many remotely connected endpoints out there today which are under almost constant attack?

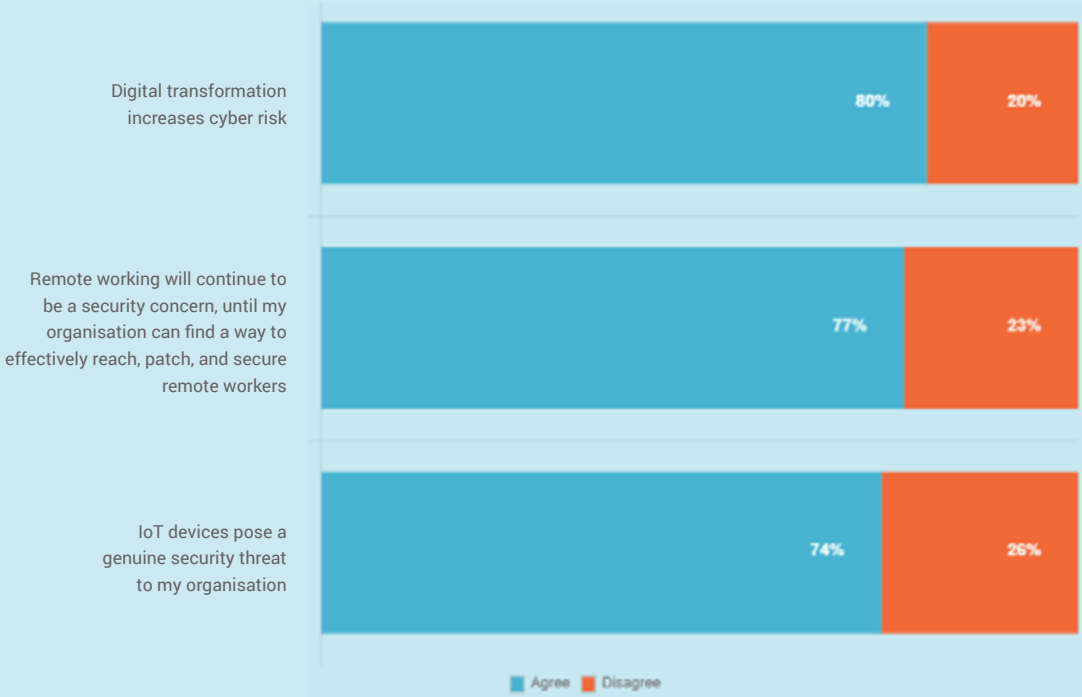
"You need to ensure that people who are not frequently on site don't become your weakest link. Patching that is only available when you're on the physical location, for example, is totally wrong. You really need to have a way of working that means that, for really critical activities, location doesn't matter."

Kurt De Ruwe
CIO of Signify (formerly Philips Lighting)

Microsoft MVP Jason Sandys says it's a behavioral issue. "Remote workers don't always have a strong affiliation to the company; the natural attachment you get from being in an office isn't necessarily there. That's a big security concern, because the average employee isn't focused on defending the network it's even tougher to get on the remote workers' agenda. Once the system is compromised, the data is compromised.

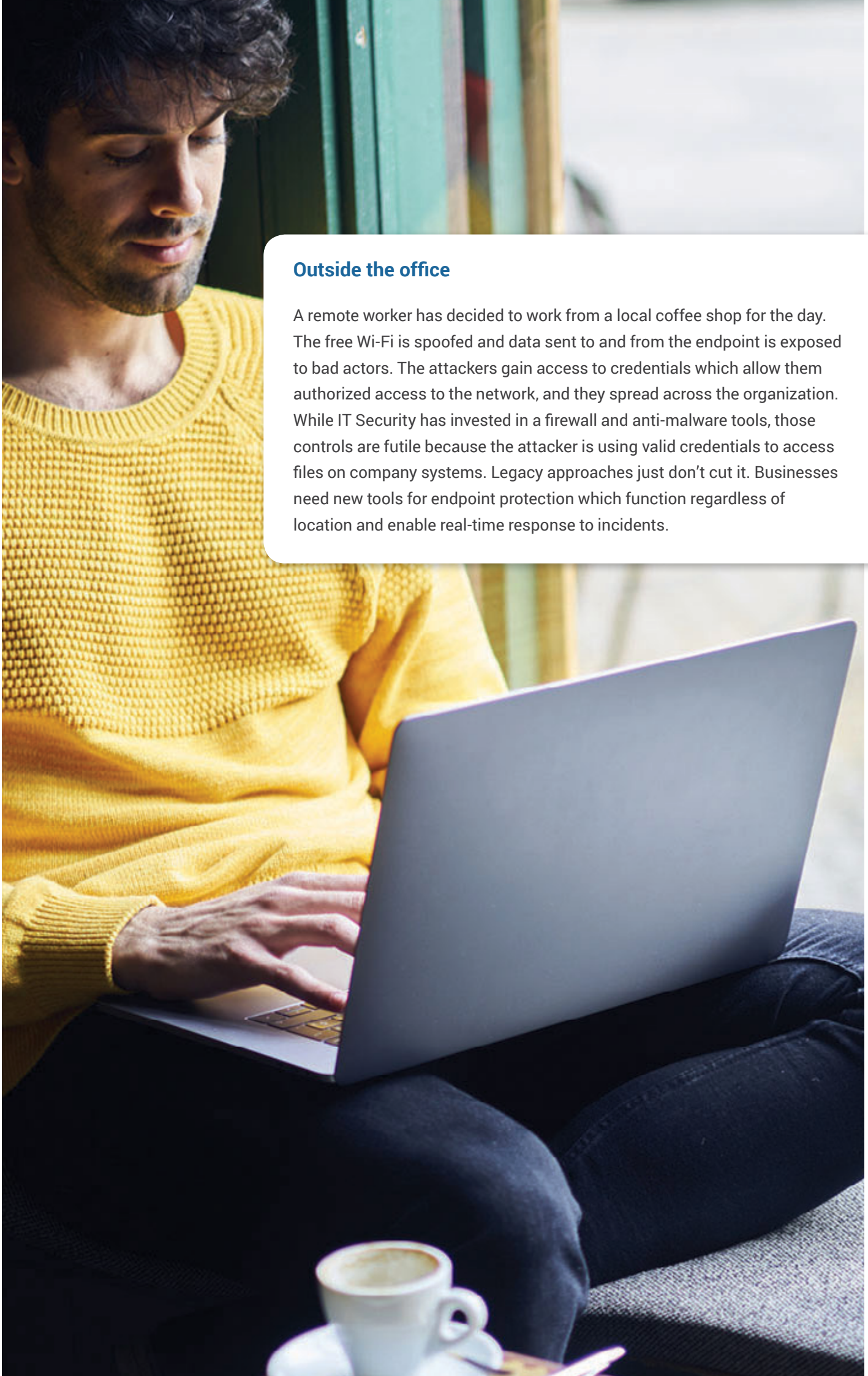
"The challenges have been there for a long time, but now you have people sitting in coffee shops, on public Wi-Fi, working on their company laptops. This is, or should be, shifting the perspective of the security boundary."

Factors Increasing Cyber Risk



Analysis showing the percentage of respondents who agree and disagree with the above statements. Asked to all respondents (600)

Source: 1E survey of 600 UK & US IT decision makers, Feb/March 2019



Outside the office

A remote worker has decided to work from a local coffee shop for the day. The free Wi-Fi is spoofed and data sent to and from the endpoint is exposed to bad actors. The attackers gain access to credentials which allow them authorized access to the network, and they spread across the organization. While IT Security has invested in a firewall and anti-malware tools, those controls are futile because the attacker is using valid credentials to access files on company systems. Legacy approaches just don't cut it. Businesses need new tools for endpoint protection which function regardless of location and enable real-time response to incidents.

The IT Operations / IT Security divide

Knocking down walls

"We often see IT Operations and IT Security using different tools that don't integrate, and therefore they don't agree on what constitutes a threat or how assets are categorized and prioritized, By removing siloed and duplicate tools, you can achieve transparency, operational efficiency and cost effectiveness. This provides a single source of truth that can guide your operational and security strategy."

Michael Daniel
Former Special Assistant to President Obama
and Cybersecurity Coordinator at the White House

Presented with the prospect of accelerated digital transformation, IT realizes that internal collaboration is vital. However, fewer than a quarter (23%) of respondents believe that the IT Operations and IT Security teams work together extremely well to secure the business, creating a significant hole in security protocol.

"It's political", says Sandys. "There's a lack of cohesion, and a disparity in objectives. IT Security thinks it's seen as the enemy; the blocker to productivity. IT Operations will push ahead with a project, but it'll be inhibited by the IT Security team, which naturally have to be cautious. This scuppers collaboration".

It's not just IT Security's fault, however. "IT Operations should understand that the security team has different objectives, and therefore different accountability", says De Ruwe. "It's good for teams to challenge each other and compromise in a pragmatic way".

Neighbors of a different nature

When considering PCs and servers, IT Security's job is to say that there is a problem, while IT Operations' job is to fix it. This is because in most organizations the change management process is owned by IT Operations, as they need to consider business use, impact on business processes, and how best to make the change.

However, our survey revealed a disturbing lack of trust in the dynamic between the two teams. Less than half of our IT Security respondents felt able to totally rely on IT Operations to cover security alerts (49%), security breaches (48%) or to keep software patched and up-to-date (47%).

With relationships strained, perceptions are skewed. Three quarters (75%) of respondents agree that the IT Operations team at their organization has a "keep-the-lights-on" mentality, focusing on availability over security. What's more, almost two thirds (62%) of respondents, feel that the IT Security team knows exactly how to make the organization more secure, while IT Operations make securing the business more difficult.

Closer alignment is a must. Respondents say better communication (62%), and/or improved sharing of data (57%) between the IT Operations and IT Security teams would help. The collaboration issue has implications for technology procurement as well. Over half (54%) of respondents feel that when it comes to the tool procurement process, their organization's IT Operations and IT Security teams only collaborate "fairly well".

"Get the two teams working together and agreed on aims, and create a shared toolset", says De Ruwe. "When something does go wrong, don't play the blame game. If you point a finger, there are usually three fingers pointing back. Use your collective energy to solve the problem instead."

Sixty-two percent of respondents feel that the IT Security team knows exactly how to make the organization more secure, but IT Operations make this action more difficult.

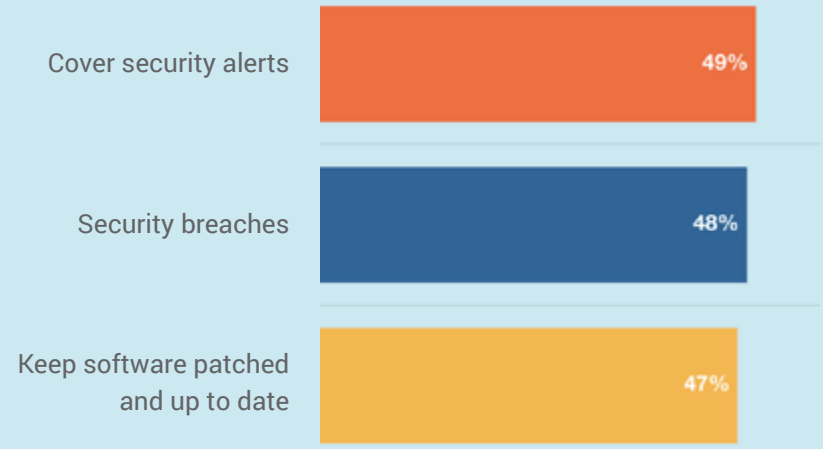
1E survey data

Friends and Neighbors

The bottom line is that nearly all (97%) respondents believe that their organization would see benefits from better IT Operations and IT Security collaboration. Perceived benefits include:

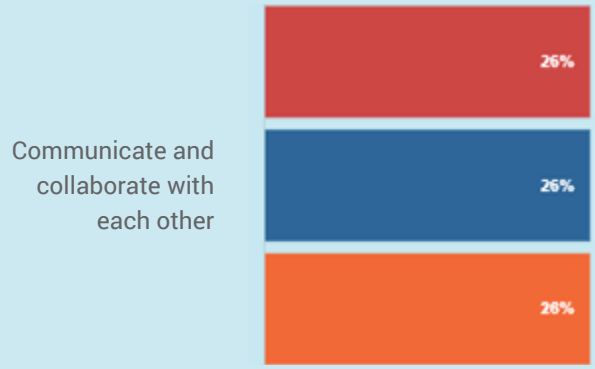
- Six in ten (59%) predict faster reaction times to security breaches as a benefit of better collaboration
- Nearly half (48%) expect a better understanding of the tools required to be more successful
- Almost two thirds (62%) foresee increased efficiency

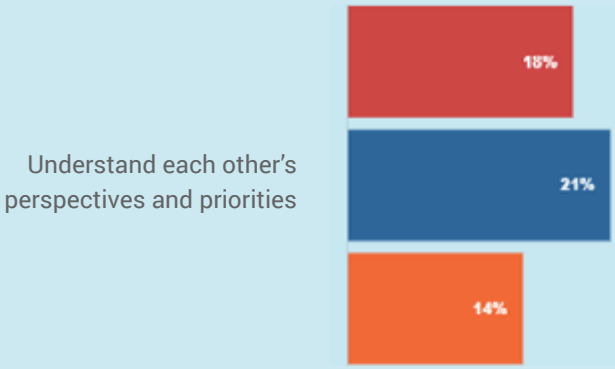
Trust in IT Operations



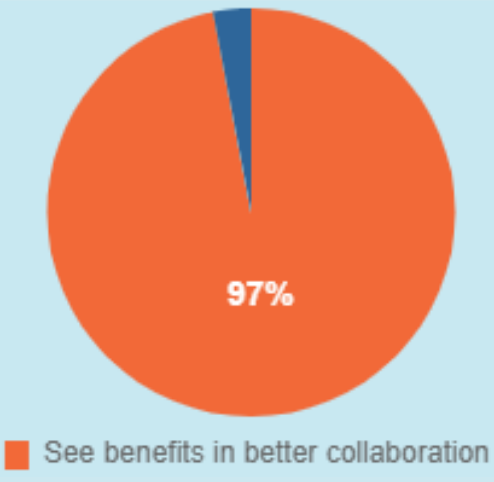
Analysis showing the percentage of respondents who feel that IT security can totally rely on IT Operations when it comes to the above areas. Asked to all respondents (600)

IT Operations / IT Security. A way to go but a will to get there





Analysis showing the percentage of respondents who believe that their organization would benefit from better IT Operations and IT Security collaboration. Asked to all respondents (600)



Analysis showing the percentage of respondents who believe that the IT Operations and IT Security teams in their organization do the above tasks extremely well – they are very good at them. Asked to all respondents (600)

Source: 1E survey of 600 UK & US IT decision makers, Feb/March 2019

The software arms race

Power tools

“We fully standardize on the Windows 10 environment, but we always make sure we are up-to-date with all the latest releases. Every single security patch – users cannot refuse it – gets installed automatically as soon as it becomes available. If your infrastructure environment is not properly managed, then you can have the greatest security tools and still have a big risk. That’s our policy: to patch, patch, patch the moment something becomes available.”

Kurt De Ruwe

CIO of Signify (formerly Philips Lighting)

Vulnerabilities and exploits are regularly made public. Once an exploit is discovered, even a tech-savvy 14-year-old can sit in their bedroom, find this information and stitch malware together to create chaos.

Most vulnerabilities targeted in attacks already have patches available. The success of exploits such as NotPetya and WannaCry, however, point to the continuing need for organizations to take more responsibility for their own defense, and ensure that all such updates are properly deployed. This is evident in our data. Respondents say that just 66% of their organizations' software estate is current, meaning 34% of endpoints remain open to exactly these types of breaches.

Just 66% of organizations' software estate is current.

1E survey data

Visibility and control

It is not fair to lay the blame on any one team, when there are fundamental issues with the tools these teams must rely on.

Our respondents reported a significant lack of endpoint visibility and control capabilities. On average, they feel that they only have visibility of 64% of their organization's total software estate. That leaves a huge literal blind spot of 36%. As for endpoint control, the figure stands at 58%. How do you protect what you cannot control or even see?

Risk, opportunity & Windows 10

The way in which operational limitations can lead to structural vulnerabilities is particularly evident around Windows 10. Respondents report that on average their organization has migrated only 68% of their machines to Windows 10, leaving some way to go until the process is complete.

This is worryingly low. Windows 10 has been available for three years – during which time criminals have largely been free to exploit vulnerabilities common in older Windows operating systems.

The improved security functions in Windows 10 are one of the reasons eight in 10 (83%) say security is a motivating factor for their organizations' migration to Windows 10. In addition, over half (58%) feel that a failure to meet the Windows 7 support cut-off on January 14th 2020 poses a significant security risk (as well as increased license costs), which may be why a similar number (56%) are worried that their migration isn't happening quickly enough.

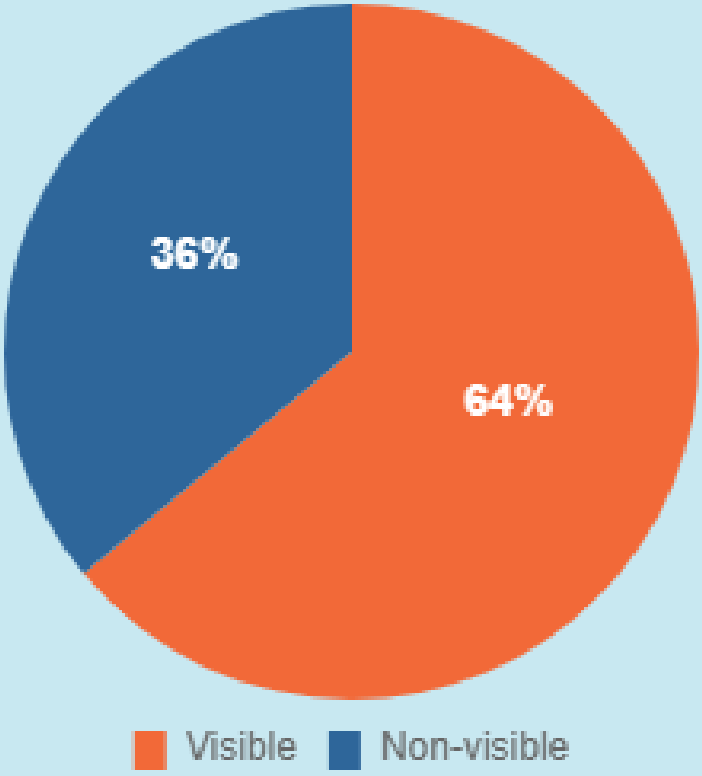
Particularly concerning for these organizations is the natural tendency to leave the most difficult migrations to last. Over 6 in 10 (62%) identify the migration of remote workers to the latest version of Windows as a challenge.

"For maximum efficiency, organizations should look to remove the need for human intervention in keeping your endpoints up-to-date as much as possible. Using automation tools to deploy patches and upgrades, and timing patches when most of the workforce isn't online (at 6AM, for example) can ensure the process works as seamlessly as possible, and it frees up IT staff to address those machines that need special attention."

Michael Daniel
Former Special Assistant to President Obama and Cybersecurity Coordinator at the White House

The Endpoint Visibility Blind Spot

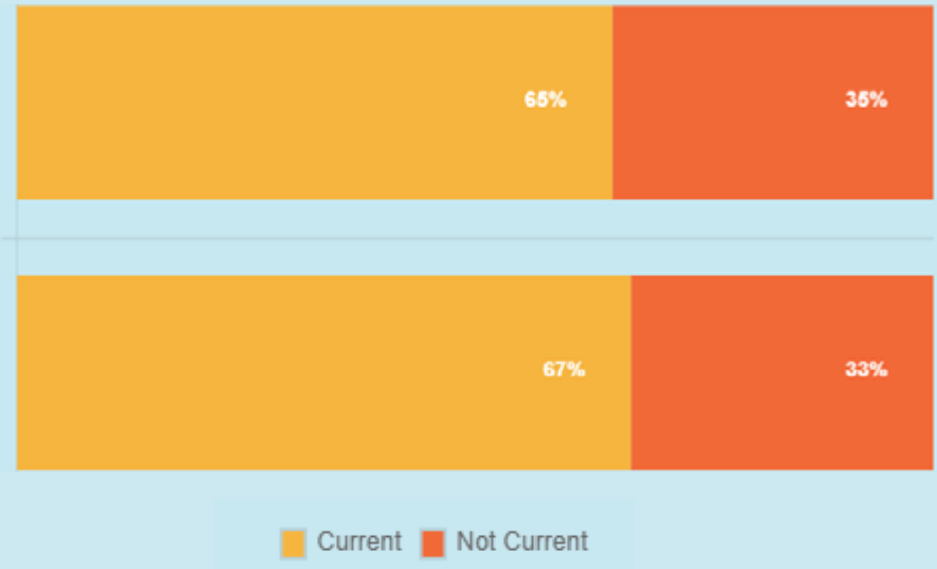
Analysis showing the average percentage of endpoints on respondents' organizations' networks that respondents have visibility of. Asked to all respondents, split by respondent focus (600)



The Software Security Threat

Average percentage of respondents' organisations' software estates that is current today

Average percentage of respondents' organisations' machines that have already been migrated to Windows 10



Analysis showing the average percentage of respondents' organizations' software estates that is current today, and the average percentage of respondents' organizations' machines that have already been migrated to Windows 10. Questions asked to all respondents (600)

Source: 1E survey of 600 UK & US IT decision makers, Feb/March 2019

On Board

Taking the issues to the top floor

"What percentage of machines are up-to-date with patching? How many are upgraded to Windows 10? It's entirely possible the board is unaware of the real risk because they don't have the complete picture. Decide on some input-based metrics, track performance and adjust or add more over time."

Michael Daniel
Former Special Assistant to President Obama
and Cybersecurity Coordinator at the White House

Taking the issues to the top floor

When it comes to budget allocation, the vast majority (90%) of respondents report that their business prioritizes other things over cybersecurity. The pressing question therefore becomes: how do we prioritize the resources that are allocated?

Our respondents believe that an increase of investment is required most in these areas: the automation of software migration (80%), breach response and remediation (67%), and/or software patching (65%).

In other words, a greater investment is called for to remedy protection through patching and automation, as well as better solutions to respond to breaches as they happen.

Gaps in understanding

Does the board realize that those entrusted with the pivotal responsibility of ensuring these doors and windows are shut (and hopefully locked) typically can't even reach or see a third of the endpoints?

Fewer than a quarter of respondents believe that their organizations' board of directors has total awareness regarding the level of control that the IT department has over endpoints (23%), and visibility possessed by the IT department over the software estate (21%).

This lack of awareness from the board carries over into the number of software licenses in use (25%), and how up-to-date the software estate is where, again, fewer than a quarter (23%) feel that there is total awareness among the board. Among respondents from the UK, perceptions of board awareness fall even lower (13-17%).

No one expects the board to suddenly concern itself with IT minutiae, of course, but better reporting practices, along with new, more meaningful performance measurements could improve both awareness and funding.

The vast majority (90%) of respondents report that their business prioritizes other things over IT Security when it comes to budget allocation.

1E survey data

Cyber Investment

Analysis showing the percentage of respondents who think that their organization's investments in the above areas of cyber security needs to increase, decrease, or stay the same over the next 12 months. Asked to all respondents (600).

Source: 1E survey of 600 UK & US IT decision makers, Feb/March 2019

Conclusion 5

A house divided cannot stand

"Real-time information makes all the difference. Today, 1E's Tachyon is so embedded in how our IT Operations team functions, that if we were to take it out, there would be rebellion."

Kurt De Ruwe

CIO of Signify (formerly Philips Lighting)

What's clear is that these issues cannot continue. There is far too much on the line, particularly when more malicious, well-funded, and organized attacks are taking place.

In total, 73% of respondents said they were more dependent on software than they were three months ago. It points to an ongoing, continuous escalation of all these problems – unless we take control of the situation.

We've seen the lack of trust around IT Operations, the lack of visibility and control they endure, and the demand for tools that enable them to reach, patch and update endpoints more effectively.

Given the increasing prevalence of remote workers, and the difficulties in securing them, it goes without saying that these tools must be inclusive of them – that means providing remote users with self-service, and giving IT teams the ability to respond to remote worker incidents and vulnerabilities in real time. Without these capabilities, significant gaps will remain.

Of course, there are ultimately several pieces that must come together, and many of them are cultural. If one of them is ignored, the business will remain unsecure. It requires strong leadership and collaboration, but the results are worth it.

Our 10-point action plan, compiled by cybersecurity expert Michael Daniel (former Special Assistant to President Obama) uses our findings to show you can make the difference at your organization.

10 Point Action Plan

Minimize your cyber risk

by **Michael Daniel**

Former Special Assistant to President Obama and Cybersecurity Coordinator at the White House

Cybersecurity and IT Operations often seem to conflict – the security people recommend actions that admins find impossible to implement, while the operations side takes actions that security sees as creating unneeded risk. However, while you can never drive your cyber risk to zero, if IT and cybersecurity operations work together, you can dramatically lower your risk profile. Here's 10 ways to do that.

1 Align goals closely with the business for pragmatic security versus operational requirements

Actions

Agree on which IT systems are most critical for business operations to determine

Identify systems that could be retired to allow for efficiency gains and reduced security requirements

2 Create shared objectives and responsibility for IT Security and IT Operations

Actions

Seek 100% asset visibility

Upgrade and patch based on an agreed set of shared KPIs (the standard 90% in 30 days is too slow)

Ensure your critical assets are patched and updated as a priority

Mitigate the resulting vulnerabilities if you can't patch or update

3 Employ a common set of tools and appliances

Actions

Remove siloed/duplicate tools for transparency, operational efficiency, and cost effectiveness

Have one (agreed upon) source of truth

4 Automate patching and updates to the maximum extent possible

Actions

Minimize the need for human intervention where possible

Enable remote workers to self-serve for OS upgrades to reduce the burden on IT

Enable operational and security tasks to be carried out in real-time on every endpoint without distracting users

5 Create transparent progress reporting for IT and Security teams

Actions

Ensure everyone can see progress towards the visibility and patching goals

6 Establish consistent reporting on security posture to the board

Actions

Develop a KPI-driven framework for board reporting that increases awareness of security posture

Make both IT Operations and IT Security accountable for the achievement and reporting of these KPIs

7 Join a cyber information-sharing organization relevant to your industry

Actions

Make sure your IT Operations and IT Security teams have access to the latest threat information

Adjust your operations and security posture based on that threat information

8 Develop a clear and shared incident response and recovery plan

Actions

Identify who is responsible for what actions during a cyber incident

Rehearse such eventualities

Integrate the technical response activities with your company's broader incident response plan (e.g., legal, public relations, etc.)

Develop the capability to recover from cyber incidents when they occur

9 Break down barriers to communication

Actions

Communicate priorities and goals from management

Physically locate IT Operations and IT Security together if possible

Incentivize regular communications between IT Operations and IT Security

10 Update your action plan, KPIs, and priorities (at least) annually

Actions

Adapt priorities to stay consistent with business needs

About 1E

Modern users expect a mobile-like experience, with self-service and instant results. 1E enables IT to deliver comprehensive self-service and respond in real-time by augmenting Microsoft and ServiceNow solutions. Over 1000 organizations trust 1E to meet their user, business, and security needs. Your employees are important; they deserve 1E managed endpoints.

Get in touch