Never pass on password security

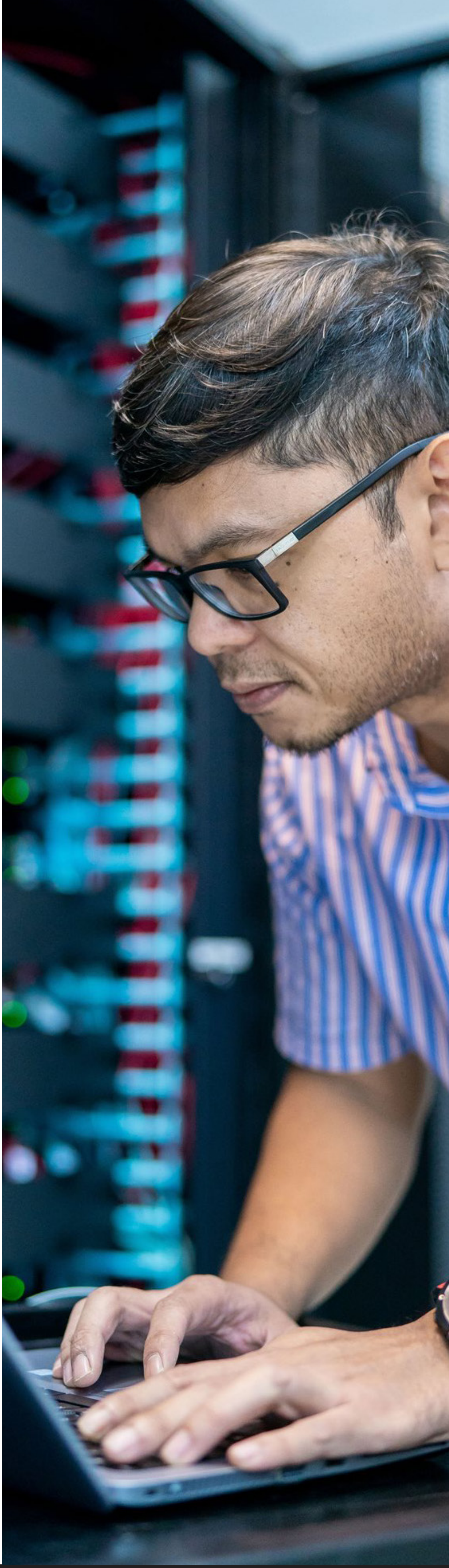
Opportunities and challenges for business transformation

Orange
Cyberdefense

Introduction

It doesn't matter which sector your company operates within or how much data it holds: risk is ever-present. Instead of viewing this as an endless battle, though, there's an opportunity for businesses to assume control by taking a proactive approach to cybersecurity. Many businesses are needlessly exposing themselves and their employees to risk, due to poor password security, a lack of cybersecurity skills, and choosing convenience over security.

These challenges were the subject of a recent roundtable event held jointly by Orange CyberDefense, a managed security, threat detection and threat intelligence services provider, and Okta, a specialist in identity and access management. The event gathered CTOs and senior figures from a wide range of public and private sector organisations to discuss how users can authenticate securely, and how best to create an environment that encourages digital transformation without exposing a business to unnecessary risk.



Part 1:

Challenges

Dumb passwords

According to one estimate, the average internet user has 200 accounts which require a password, a figure which is set to double over the next five years. We perhaps shouldn't be surprised, then, that users re-use passwords. In the words of one CEO attending the roundtable event:

> **Things haven't changed for 30 years: we're still talking about the same things and we're still just typing 'password'!**

Breach analysis by the UK's National Cybersecurity Centre found that 23.2 million victim accounts worldwide had used '123456' as their password.

> **We need to stop IT teams from re-using passwords or having the same password as a user than they do as an admin.**

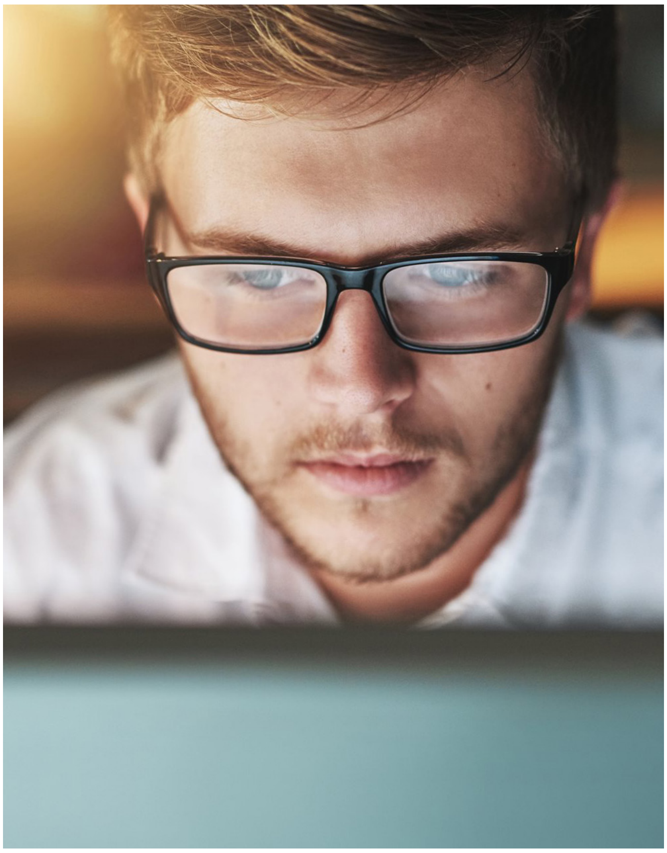
The comment from one attendee at the event. Even major global organisations are fallible: following the Maersk NotPetya attack, an independent cybersecurity researcher discovered a ship in South American waters was using default credentials (the username 'admin' and password '1234') to secure its satellite communications systems – in effect, presenting an open and unlocked door to hackers!

The response by many companies to poor password security has been to introduce stricter password and access controls. However, this introduces a further challenge: balancing ease of access with a robust level of security.

The IT user: friend or foe?

According to one estimate, around two-thirds of data protection and privacy training professionals labelled their employees as the 'weakest link' in terms of protecting their firm from cyber threats. This sentiment was reflected at the event, with a senior figure from a public sector firm admitting that "We [businesses] don't treat our users as customers, we treat them as an annoyance".

By failing to take into consideration the service needs of users (such as easy, efficient authentication), many resort to downloading unauthorised applications on their enterprise network. This use of shadow IT is pretty widespread: according to a 2019 report, 67% of end users or teams have introduced their own collaboration tools to their organisation, without IT team sign-off.



The cybersecurity professional

It may be easy to point the finger at users, but the reality is, we can't tackle cybercrime without a strong workforce of cybersecurity professionals. And therein lies challenge number three. Despite cybersecurity being one of the most highly-paid specialised areas in technology, there's a significant dearth of necessary skills. An attendee at the event representing a charity-sector firm shared his company's frustrations:

> **We're constantly hiring, but universities aren't exactly chucking them [cybersecurity professionals] out. There's a lack of security talent, and the current generation of cyber professionals are retiring, so a lot of the workforce will be lost.**

It's little surprise therefore that there are almost three million unfilled cybersecurity positions worldwide. Compounding these issues, according to attendees at the event, is the defection of "really smart guys" from cybersecurity to areas like AI and ML.

Security vs convenience

Even if the talent is available, buying new software to bolster security and authentication could be perceived as having a negative impact on the user experience or brand reputation. On the other hand, failing to invest or investing in only basic authentication tools (which may appeal to users who expect application access on-demand), will come at the expense of security.

Getting the cost-convenience-security dynamic right is crucial, but not always easy in an organisation where requirements, expectations and objectives of different departments differ wildly.

A senior figure from an international sports brand gave the perfect example, he said, "My company has so many different entities. IT wanted to take the website down [to protect users], but the CEO wanted to keep it running [to protect the brand's reputation]".

Part 2:

Solutions

Learn from your mistakes – and from others'

Enterprises should look to identity and access management solutions that can be easily integrated into workplace apps, making the additional level of security undetectable to users (and thus more convenient). Single-sign on, supported by one-time-passwords, allows users to securely access all apps on a single dashboard. Already deployed in one healthcare service, the attendee from a sub-sector of the organisation advised, "if there's one thing you do to increase security for your business – implement single sign-on."

Being a target of a breach is a likelihood for most companies, so how they deal with events and what they learn are important. An attendee heading up security at a law firm said, "I'd encourage everyone to be open if there's been a problem. Regulators will give you a lot more slack, rather than just slamming the door – and your clients will likely take a similar approach".

It's possible to extract some value from damaging incidents, including assessing breaches as if they'd targeted their own business. The security figure from the healthcare organisation shared an example of this strategy in action, explaining that, following the hack on British Airways, "He ran the incident based on that [British Airways] scenario to try and display gaps and weaknesses in our own architecture." He went on to say:

> **I found that this particular scenario could have happened to us. It's important, as cyber professionals, to look at this free information and take collective responsibility.**

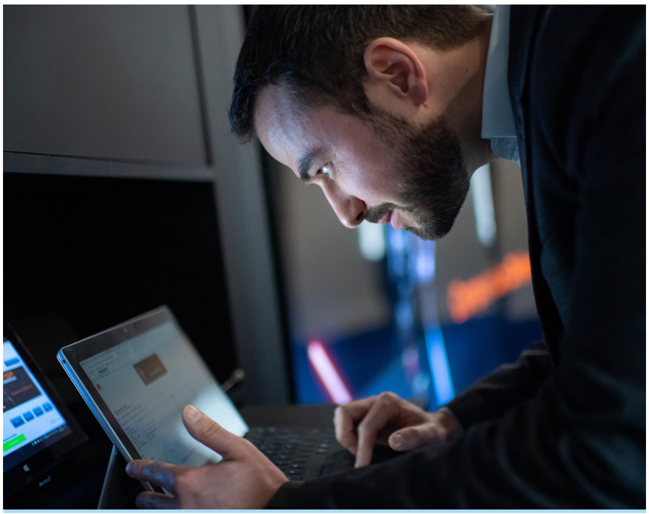
Value can also be found in the wealth of free advice available online, such as the UK's National Cyber Security Centre (NCSC) and the European Union Agency for Cybersecurity (ENISA).

Self-audit

Any security strategy should begin with a full license audit: you can't manage what you don't know about. Assess who has access to what, and what kind of access they've been granted. This must include, according to an event attendee from a not-for-profit organisation:

> **Cloud auditing: you'd be staggered by how many cloud services your employees use. The endpoints and applications you think you need to secure will be just the tip of the iceberg.**

Again, implementing single sign-on can be of great help, reducing the complexity of having to manage multiple user identities across siloed solutions. This is particularly important when an employee leaves a firm. The solution, commented an attendee, "is to integrate security processes with HR processes." HR professionals are not tech experts. As such, implementing strict security policies must involve tools which allow HR figures to manage user profiles, groups and devices (as well as assign rights) via a single, user-friendly admin console.



Outsource to improve

Trends in cybersecurity spend are shifting, as more businesses understand the value of managed services over hardware. A recent report showed that in 2018, spending on security services overtook that on products, with security services expected to represent at least 50% of security software delivery by 2020.

This was supported by commentary from event attendees, including the individual from the healthcare department, who summarised the evolution of the organisation:

> **We used to focus on technology, but now we're shifting that focus to people and processes.**

Most companies don't have the required resources in-house, so outsourcing is a necessity. Instead of a focus on siloed technologies to mitigate risk, the right teams will address cybersecurity as a whole, providing a range of solutions that assess risk, detect threats, protect IT assets and respond to security incidents.

Don't let cybersecurity become a people problem

Change must also come from within. Employees must be alert to phishing scams and adopt strict password practices. Teams should have a basic understanding of IT infrastructure, applications and internal networks, as well as common tactics, techniques and procedures used by hackers. Training courses are often available from managed security services providers, and enable businesses to reduce risk by promoting collective responsibility for cybersecurity.

Finally, change must also start at the top, with buy-in from the c-suite. Communicating cybersecurity threats can be a challenge.

"They think the rules don't apply to them," admitted one attendee at the event, who explained that this is not always the fault of the c-suite, as too often "we talk in terms execs don't understand." The solution championed here was simply to involve senior management.

> **It really rings home when you show him [the CEO] his inbox. This works really well: we crack his passwords and present how easy it is to access his accounts. We talk in a language they get.**

Conclusion

Workforce and customer identity are crucial to the security of a business and therefore the success of its digital transformation. Password re-use is the biggest danger within most organisations, and single sign-on is one of the easiest ways of minimising risk. Businesses must remain open and transparent, and share knowledge and experiences to educate others.

Things might not have changed much over the past 20 years, but that doesn't mean that transformation is impossible. Organisations can reduce risk while maintaining a seamless user experience, by implementing the right tools, working with the right people, and educating the entirety of their workforce. And, of course, by never "just typing 'password'."

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to protect freedom and build a safer digital society.

We are threat research, intelligence-driven, offering unparalleled access to current and emerging threats. With a 25+ year track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world and sales and services support in 160 countries, we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

We embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. It is our people that make us different.

We are proud of our high-end security research unit, thanks to which we publish regularly white papers, articles and tools on cybersecurity which are widely recognised and used throughout the industry and featured at industry conferences including, Infosec, Manchester DTX, RSA, BlackHat and DefCon.

Orange
Cyberdefense

orange™