sekuro

A Human Perspective On ZERO TRUST

Lee Roebig
Jason Trampevski

Table of Contents

Introduction	1
What is Zero Trust, Anyway?	2
Zero Trust – It's Not Just About Systems and Networks	3
How Zero Trust Can Be Applied to People	4
How Can We Give People More Context?	5
How Can We Convince People to Take Notice?	8
Problem 1: A Lack of Cyber Security Understanding	9
Problem 2: A Bad Impression of the Cyber Security Team	11
Problem 3: A Lack of Incentive	14
Takeaways	16

Introduction

It's no secret that human error remains one of the highest risks to an organisation's cyber security posture in today's world.

In fact, a study by Mimecast revealed that **91% of attacks today began with a phishing or spear phishing email.** Now, there are multiple tactics/technologies to reduce this risk such as MFA, SSO, ABC, SEG, ICES, UBA, 123, SAT and many other rather confusing acronyms (by the way, two of them are made up – guess which ones). Many of these can be quite effective, but they often miss getting to the core of the problem – understanding humans themselves.

Once we peel back the layers of what motivates people to change their behaviour, we can approach these human-based-risks strategically with outcomes or architecture first, and technologies and tactics second. Many organisations make the mistake of doing it the other way round (throwing technology at a problem before understanding how they will truly change people's behaviour or mitigate human based risk). Which leads to confusing architecture, high costs and low value delivered.

But what should an organisation look at when it comes to a modern security approach that adequately address human based risks whilst encouraging behavioural change? We believe a philosophy and strategy aligned with Zero Trust and its principles can be utilised in this way to truly make people change their behaviour, whilst backing them up with layered defences in case of a failure.

This e-book will look at the human elements an organisation must take into account when building a modern cyber security strategy, how Zero Trust fits in and what actions organisations can begin taking today.

01

What is Zero Trust, Anyway?

We don't blame anyone for asking this question. The market has not done the best job of explaining it, its benefits, or how to use it (apart from buying something new, of course). This has unfortunately led to a lot of cyber security and technology leaders brushing off the term as merely the latest buzz word, full of smoke and mirrors with a sales agenda. Let us try and clear the air and explain it agnostically:

Zero Trust is the concept that no-one and no thing, (whether that be a network, user, device, application, server etc) has access to anything until proven they should be trusted. And we must take as much context into account before making any **trust decision**.

If that's too long, here's a shorter version: "Zero Trust – More context with minimal assumptions before granting access." As you can see, the term "Zero" in "Zero Trust" is slightly misleading. We can't literally have Zero Trust – because that be locking everything off and not letting anyone do anything! Although that would be good for security, we don't know how long the CISO would last in that business.

02

Zero Trust – It's Not Just About Systems and Networks

So we've identified what Zero Trust is – it's about understanding more context about what is happening surrounding a request, before we trust and grant access. When many people hear that – they start to jump into ideas like:

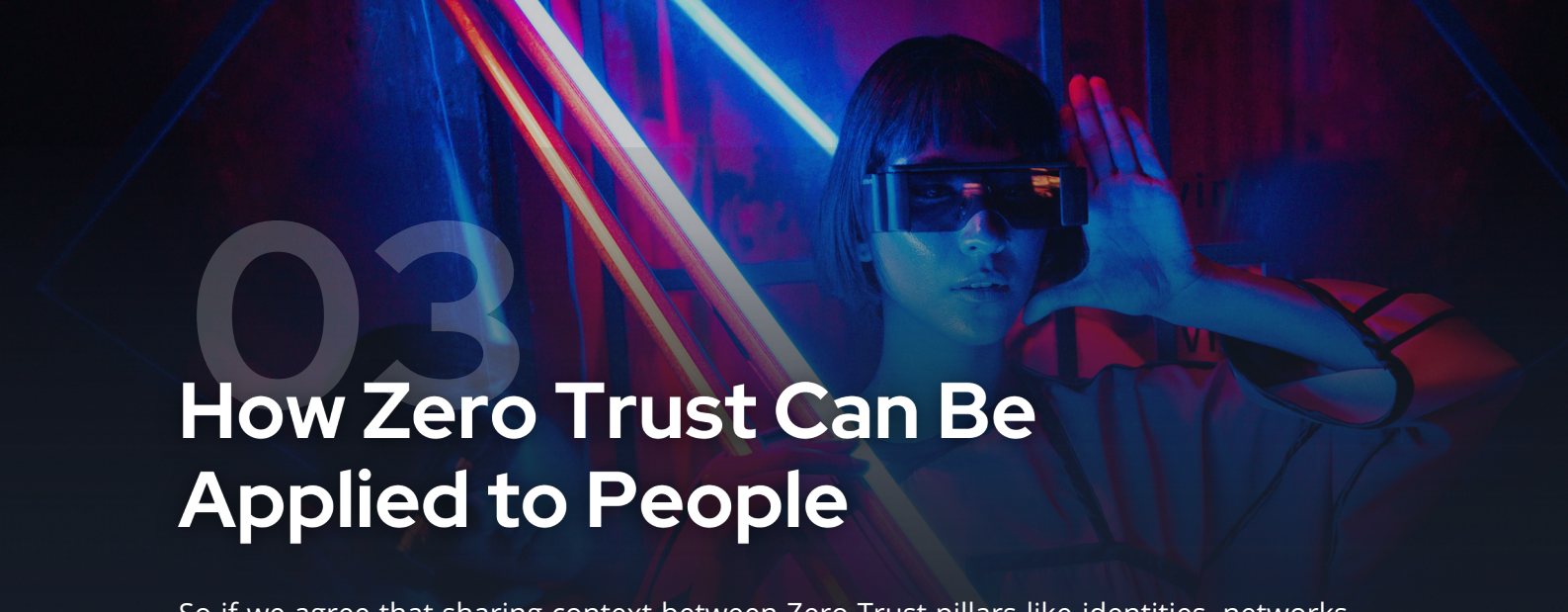
> "That means our Identity system should talk to our Anti-Malware and Device Management systems before we grant access to resources, to ensure only secure devices are granted access to sensitive applications."

OR

> "That means our network shouldn't trust based on user IP addresses, but rather their device state, identity, MFA and map them to specific IPs/ports on a per user basis."

If you're thinking of those type of examples – you're on the right track to how some aspects of Zero Trust can be implemented in terms of identities, networks and endpoints.

But there is a problem. Those things have nothing to do with why you're reading this e-book. We're here to discuss Zero Trust in relation to **people**.



03

How Zero Trust Can Be Applied to People

So if we agree that sharing context between Zero Trust pillars like identities, networks, applications and endpoints allows systems to make better decisions about what to trust, we can take the same principles and apply it to our people. If we can give our people more context in the decisions they make regarding trust, they can also make better decisions on what to trust.

You may think 'trust decisions' and 'access decisions' only apply to what servers and infrastructure do, but that's not the case. Our people make trust decisions all the time, such as:

- **When they click on a link**
- **When they open an email**
- **When they answer the phone and action a request**
- **When they browse a website**
- **When they enter their credentials**
- **When they transfer money**
- **Where they upload data**
- **Who they share data with internally**

If any one of these trust decisions is made with poor judgement, the impact can be the same (or worse) as when an attacker gets access into a network or infrastructure.

This leaves us with two important questions:

- How can we give people more context before they make these types of decisions?
- How can we convince them actually take notice and want to make better decisions around cyber security?

04 How Can We Give People More Context?

To give people more context before they make trust decisions, we need to focus on effective education and communication strategies whilst incorporating technologies such as MFA, SSO, SEG, ICES, UBA, and SAT (don't worry, we'll explain what those are in plain English below). Here are some methods to provide our people more context before they make each trust decision:

When they click on a link

- **Implement Security Awareness Training (SAT)** that teaches employees to recognise suspicious links and websites, and communicate the potential risks of clicking on untrusted links. Many SEGs (Secure Email Gateways) have capabilities to sandbox links before they can interact with the end user.
- Additionally, for certain potentially risky domains such as Newly Registered or Uncategorised, **display a warning to the users before they can proceed**.
- Finally, **encourage the use of Multi-Factor Authentication (MFA)** to protect their accounts in case they accidentally click on a malicious link. Don't forget to measure this as often as possible through regular phishing tests to make sure your SAT program is working the way you desire.

When they open an email

- **Use Secure Email Gateways (SEG) and Integrated Cloud Email Security (ICES) solutions** to help filter out phishing emails and other malicious content.

- **Train employees to identify phishing emails and emphasise the importance of single sign-on (SSO)** to minimise the risk of credential theft.

- **An ICES/SEG can be configured to also provide warning banners** to employees if an email came from externally, and if the email domain or sender address is remarkably similar to internal staff, whilst being actually different.

When they answer the phone and action a request

- **Develop guidelines for handling phone requests and require employees to validate the identity of the caller before taking any action.** This is particularly critical in payroll and finance departments, where invoice fraud is often occurring over the phone.

When they browse a website

- **Provide SAT on safe browsing habits and how to identify secure and insecure websites.** Leverage technology such as a secure web gateway (SWG) that help identify malicious websites and block access to them.

- Once again, for certain potentially risky domains such as Newly Registered or Uncategorised, **display a warning to the users before they can proceed and use Browser Isolation capabilities through your SWG to 'pixel stream' the website in a remote browser without giving the site access to the user's endpoint.**

When they enter their credentials

- **Teach employees about the importance of strong, unique passwords and the use of MFA** to protect their accounts.

- **Implement SSO to simplify the login process and reduce the risk of password reuse across multiple accounts**. Unique, user-chosen login pictures are often an option as well to help users identify whether they're logging onto the actual legit corporate identity login page or not.

When they transfer money

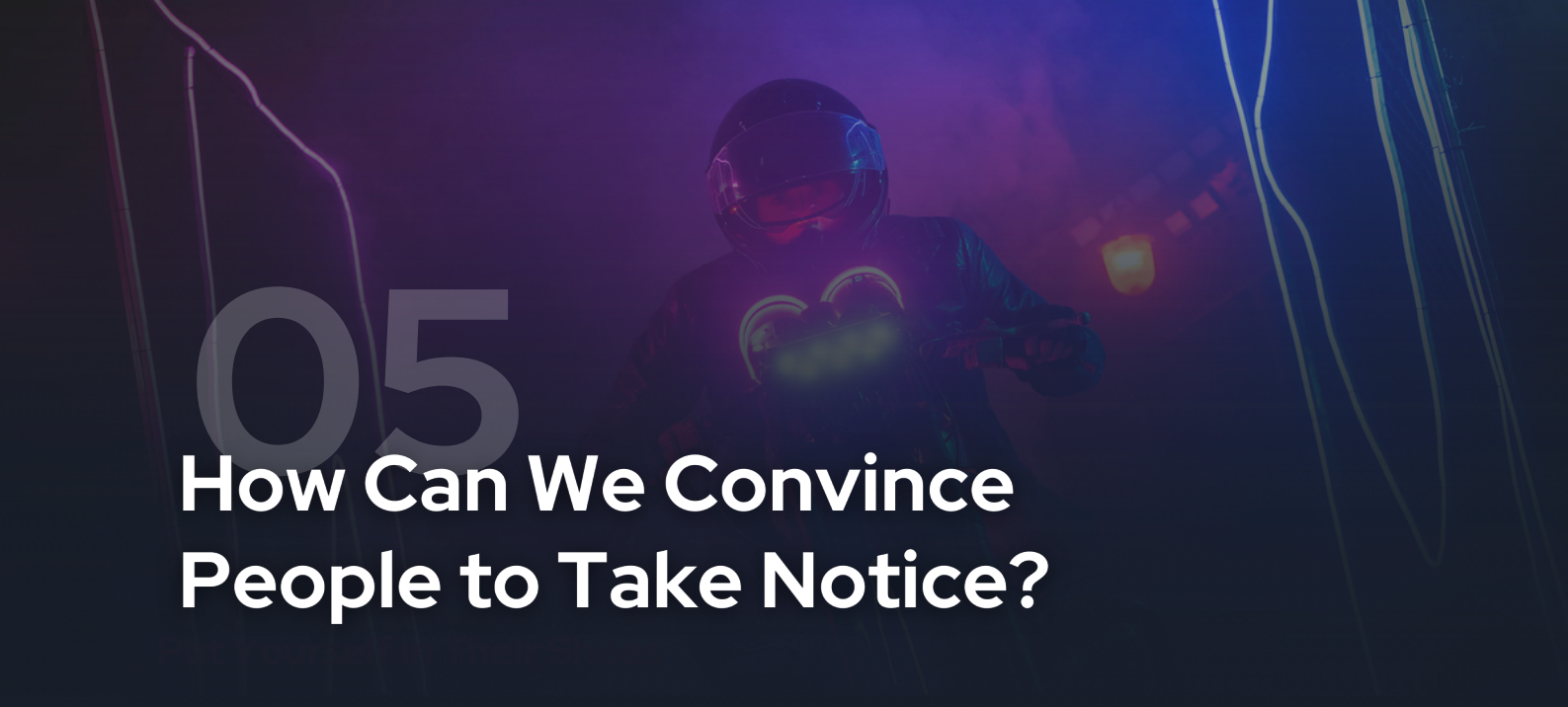
- **Establish clear protocols for financial transactions, including the use of MFA and SSO for account authentication.** Require multiple levels of authorisation and verification before approving transactions.

Where they upload data

- **Create guidelines** for securely storing and sharing sensitive data.
- **Leverage user behaviour analytics (UBA)** to monitor and detect unusual activities, such as unauthorised data access or sharing.
- **Look at integrating inline CASB into your SWG** so that you can coach/control users in real time when they upload data to places other than your corporate instances and corporate sanctioned apps.
- **Ensure your Data Sharing and Data Storage policy are hyperlinked** in any coaching messages as well, there's no better time to educate your employees than right after they've breached a policy.

Who they share data with internally

- **Develop policies for data classification and sharing** within the organisation.
- **Train employees on the proper handling of sensitive data** and the importance of only sharing information with authorised individuals.
- **Implement UBA to monitor and detect suspicious data-sharing activities.** Additionally, use an out of band CASB to look at where data is shared externally from your OneDrive, Google Drive, Box or similar services. Commission policies that will swiftly reverse an unauthorised share and send the user an email reminding them of the correct practice to follow.



05

How Can We Convince People to Take Notice?

Put yourself in their shoes

We know that no matter how much technologies, controls and policies we throw at our people, it is still ultimately within each individual person's full control on how much they intake, retain and comply with. Many cyber leaders are frustrated when despite efforts, the wider user base continues to make mistakes. Instead of frustration, leaders should put themselves in the person's shoes and try to understand the key reasons behind their failed attempts to reach their desired audience.

We believe inside organisations, there are 3 key issues that make it difficult to reach and educate our people to be cyber aware:

- **A lack of understanding of the importance of cyber security**
- **A bad impression of the cyber security team due to past experiences**
- **A lack of incentive to comply and follow cyber security policies, standards and procedures**

So, consider this turntable scenario:

If you were expected to comply with something that you did not understand, were not rewarded for, by people whom you didn't think had your best interests in mind - **would you want to comply? The answer is most likely not**.

Let's discuss some strategies that can be used to alleviate issues or completely solve the 3 problems listed above.

PROBLEM 1

A lack of cyber security understanding

When cyber leaders become aware of this issue, they often go straight to "We need to force people through more awareness training". They'll then assign more than 10 new courses to their wider user base and start badgering them for not completing them on time.

If you have been doing awareness training and none of it is sticking, **the answer is not 'do more of it'**. Remember our friend Albert Einstein's definition of insanity: "doing the same thing over and over and expecting a different result". It's time to take a step back and look at why it might not be sinking in. Ask yourself:

- Are you using pre-canned material or is it customised to your organisation? Pre-canned material will never work as effectively as tailor-made (or at least adjusted) content.
- Who are the people in your workforce you're trying to appeal to? Things like age/generational demographics and the industry they work in are critical in the tone of your content.
- What is your company culture? Is it serious and corporate or more playful/relaxed?

If you have been doing awareness training and none of it is sticking, the answer is not 'do more of it'. It's time to take a step back and look at why it might not be sinking in.

Continues in the next page

PROBLEM 1

A lack of cyber security understanding

Some key examples are:

For an organisation that works in Law: Perhaps your content should be focused on culpability from a legal perspective if data is mishandled, and what laws apply. On top of this, consider a more serious nature in your content. They may prefer content delivered in a training system, as compliance is a key focus in their jobs most likely.

For an organisation based in Retail: Your content would likely be more playful in nature, using humour. Depending on age demographics, memes are a great tool. These more casual audiences may prefer content delivered over email, but more often and in smaller, bite-sized chunks.

In summary: Understand your people, appeal to their tastes, make the content relevant and measure the success rate continuously through phishing tests, email click-through rates and course completion adherence.

Don't hesitate to adjust when things are not being successful, as it will take some time to find the right balance for your organisation.

PROBLEM 2

A bad impression of the cyber security team

"Principle of Least Privilege" – One of the most important fundamentals in cyber security. It's the act of giving any user, program, or process only the bare minimum privileges necessary to perform their role. Seems sensible, right? Indeed it is – but sometimes cyber security professionals take it too far.

Cyber security professionals often take the principle of least privilege at face value and fall into the mindset of "If they don't need it (or if we don't think they need it), I'm going to block it". An example is with their web filtering rules – blocking categories such as 'Shopping' and 'Streaming Media' without any direction from Human Resources departments. Many do this because of following the 'principle of least privilege' concept.

No doubt, it is a valuable and essential concept, but 'privilege' is the key word here. The 'privileges' we should be focused on reducing are ones that have security implications. Is watching YouTube at work a privilege with security implications? Probably not. But is there reasonable likelihood that someone will need to watch YouTube for a work-related matter? In today's world, absolutely. Therefore, there is little security benefit for blocking YouTube, but a strong productivity impact and compromised user experience.

Cyber security is most effective when seen as the "Protector" rather than "Enforcer" inside an organisation.

Remember that cyber security is most effective when seen as the "Protector" rather than "Enforcer" inside an organisation.

Continues in the next page

PROBLEM 2

A bad impression of the cyber security team

We can't be everywhere at once, so we need to create a culture where employees want to willingly approach us for guidance. We also want them to listen to us when we say something is serious or distribute a new policy or awareness campaign. If we are blocking them on matters that aren't security risks, we are controlling them for the sake of it, without having a positive outcome for the organisation's security posture. If we keep blocking them for legitimate behaviour, we become the 'boy who cried wolf'. If a system is oppressive, users will get frustrated and work around it: like choosing to disconnect from the network, use a personal device or email data to their personal account to "get real work done".

These workarounds essentially turn security to 'zero'. And who can fault their actions if the systems given to them are blocking them from performing legitimate work?

Cyber security leaders should ensure they and their team have empathy around how they architect a security solution or choose to mitigate risks. This can be done by asking:

- How serious is this risk? If it's not highly serious, going straight to blocking doesn't seem logical or fair.
- If it is serious, what would be the impact on our people if we went straight to block? (See "Put yourself in their shoes" chapter).
- On top of using our own empathy to decide, who can we talk to in each department to determine that impact?
- If the impact on people's productivity or quality of life would be high, can we find a way to constrain it fairly, instead of blocking it?
- If we can't constrain it fairly, perhaps it's time to look into a solution that can constrain it fairly.

Continues in the next page

PROBLEM 2

A bad impression of the cyber security team

Example:

We see employees accessing Dropbox. This is not a corporate application and we're concerned this could pose a threat to our data via leakage.

We think about blocking it, but then **we put our empathy hat on**: we consider that many other businesses would probably use Dropbox to send our people files. If these got blocked, our people may become frustrated and resort to less secure means.

We decide that blocking Dropbox is not a fair action, and instead look at our existing solution to see if it can block Uploading to Dropbox, without Blocking access or Downloading. Once we implement this, we have mitigated our risk of data leakage, whilst preventing productivity losses.

Remember that we are all human. Humans like to listen to people that they like and respect. If they do not **like** the security team, they won't listen to our guidance – no matter how important or logical the advice.

Let's change that by using empathy to inform our security decisions.

PROBLEM 3

A lack of incentive

What do Sales teams get measured by? You guessed it – sales targets. What do finance teams get measured by? Money saved, spent and moved around the organisation. We could go through many other departments, but we get the point: people's success are measured by the results tailored to their respective department. And thus, they do those things very well. People's full time jobs are focused on achieving the targets set forth by their leaders, and the business enjoys the positive outcome as a result.

We've long focused on the stick instead of the carrot approach in cyber security. If a user clicks on an email, it's "Bad job, back to the compliance module for you". Given the high rates of phishing success in organisations still to date, we'd say the 'stick' is not doing its job. In fact, it may be having the opposite effect of breeding disdain for the cyber security department (See the previous problem "A bad impression of the cyber security team").

So, it's time to try the carrot instead. Can we find a way to reward people for good behaviour, thereby encouraging others to do the same? If you read the previous section, we already established that people who feel respected and like the security team will have a much higher chance of listening and complying. Certainly, reward based incentives could help get them on our side.

But how would we do that?

It's time to try the carrot instead. We need to find a way to reward people for good behaviour, thereby encouraging others to do the same.

Continues in the next page

PROBLEM 3

A lack of incentive

We have seen the below work quite well, and suggest organisations look into doing some or all of these:

Form Relationships with the C-suite and Department Heads

Use industry statistics with dollar figures to highlight the importance of managing risk adequately. There are plenty of real-world stories of organisations in our own back yard suffering enormous consequences off the back of cyber breaches, so cyber leaders have a lot of choice to pick from as examples.

Leadership Buy-In

Once your senior leadership understands the importance of cyber security, convince them to add cyber security metrics in their team's KPIs or attach other reward-based systems based on results measured by the security team (reports of phishing emails, security training completed etc.)

Hold Interactive Training Sessions

This means a real person from your cyber security team holding the training sessions. Invite everyone in the organisation and offer food or snacks to all those that attend. Interact with your audience and have prizes for those who can answer questions. If you don't have the resources for this, outsourcing is an option – just make sure it's tailored for your audience.

Takeaways

- **Zero Trust is a modern approach** to cyber security that can be used very broadly across Identities, Endpoints, Networks, Infrastructure, Applications, Data and Analytics, but don't forget it can (and should!) be used for your people as well, using the tactics and techniques in this e-book.

- Approach your cyber security controls and decisions with **empathy and fairness.**

- Ensure cyber security is well respected in your business **by being respectful to those in your business.**

- Train your people regularly (not just once a year) with **tailored** and (if possible) **interactive** training. **Reward attendance instead of punishing.**

- **Measure the success of your people security program** by doing regular offensive security exercises like phishing tests and social engineering (monthly is a great cadence).

- **Adjust your cyber security awareness programs based on the success you're measuring**. If it's not working, change it.

- **Understand the types of threats and risks faced by your employees**, and the systems, tools, and processes they use daily to help identify what is needed.

Authors' Note

With more than two decades of combined experience in the cyber security trenches, we wrote this book not only from the point of view of industry best practice but also from our own know-how accumulated over the years.

It's a privilege of expertise to be able to share what you know, so we're always happy to talk to people about cyber crime, Zero Trust, and the complex world of IT security.

Every organisation's Zero Trust strategy is unique by necessity, so new challenges are always arising. If you've got questions about what you've just read, please reach out to us, and we'll be happy to give you answers.

You can contact us - Lee Roebig and Jason Trampevski - at Sekuro: **www.sekuro.io**

Authors' Profiles

LEE ROEBIG

Customer CISO, Sekuro

Lee is an experienced Cyber Security professional with 16+ years in the technology Industry. He has previously worked in cyber security leadership and architecture roles inside multiple global organisations prior to joining Sekuro. At Sekuro, Lee helps clients with Cyber security strategy, Zero Trust, Virtual CISO, mentorship, executive advisory and security architecture. He has worked with numerous clients on cyber security strategies across industries such as health, insurance, construction, manufacturing, and leisure, including multiple ASX-listed companies.

JASON TRAMPEVSKI

Field Chief Technology Officer, Sekuro

With over a decade of project experience, Jason, Field CTO at Sekuro, has honed his skills as a strategic technology leader, helping organisations achieve their broader objectives through the effective use of technology. Whether it's building resilience or driving business success, he understands the critical role that the right capabilities play in achieving these outcomes. As a specialist in translating complex business requirements into technology solutions, Jason focuses on the critical elements of people, processes, and technology. By reducing complexity and ensuring these elements work together seamlessly, he helps organisations stay agile and competitive in today's rapidly evolving digital landscape.

About sekuro

Sekuro is a cyber security and digital resiliency solutions provider that helps CIOs and CISOs take a strategic approach to cyber security risk mitigation and digital transformation. Operating at the intersection of the digital technologies and cyber security industries, Sekuro reduces cyber risk while new technologies are adopted – ultimately building business resiliency and enabling fearless innovation.

Learn more by **visiting our website**.