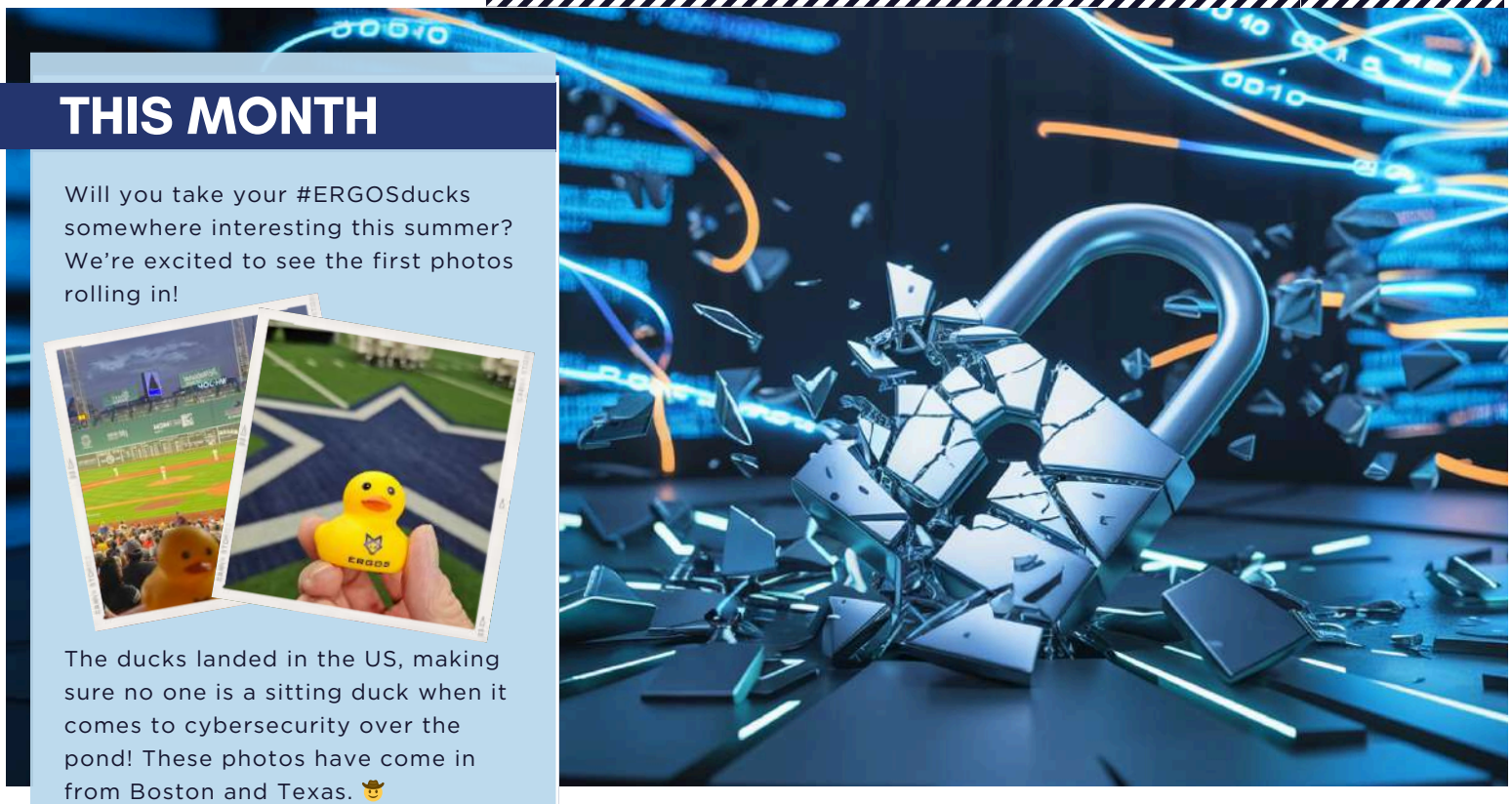
THE TECH CHRONICLE

Insider tips to make your business run faster, easier and more profitably



THIS MONTH

Will you take your #ERGOSducks somewhere interesting this summer? We're excited to see the first photos rolling in!

The ducks landed in the US, making sure no one is a sitting duck when it comes to cybersecurity over the pond! These photos have come in from Boston and Texas. 🤠

Share your photos, who knows - maybe the ducks will decide to reward their favourite ones.

This monthly publication is provided courtesy of Gino Choucair, CEO of ERGOS.

OUR MISSION:

Ensuring your technology success, securely & simply.

WHAT DO YOU DO WHEN A COMPANY COMPROMISES YOUR DATA?

With the rise in cyber-attacks worldwide, you've likely received more than one notification from a company you work with informing you that your data has been compromised in a breach. While there are steps we can take as consumers to protect ourselves, sometimes we can't control when a company that promised to protect our personal data gets hacked.

In 2023, Statista reported that 52% of all global organization breaches involved customers' personal identifiable information (PII), making your personal data – addresses, numbers, names, birth dates, NINs, etc. – the most commonly breached type of data. A recent example is US-based ChangeHealthcare, breached in February of this year, or the cyberattack on NHS just this June. Due to the February breach, it's estimated that one-third of Americans had sensitive information leaked onto the dark web.

So now what? What do you do when you receive an email from your health care provider or favourite retail store admitting, "Whoops, we got breached." It's more than upsetting to think that your data is now in the hands of criminals. When sensitive information leaks, you'll have to do some recon to protect your accounts from suspicious activity.

continued on page 2...

...continued from cover

Follow these seven steps to stop the bleeding after a company fails to protect your data from being compromised.

What To Do After Your Data's Been Leaked

1. First, make sure the breach is legit.

One ploy that hackers use to get our data is to impersonate popular companies and send out fake e-mails or letters about an alleged breach. Whenever you get a notification like this, go to the company's website or call the company directly. Do NOT use information in the letter or e-mail because it could be fake. Verify that the company was hacked and which of your data may have been compromised. Try to get as much information as possible from the company about the breach. When did it happen? Was your data actually impacted? What support is the company offering its customers to mitigate the breach? For example, some companies offer yearlong free credit monitoring or identity fraud prevention.

2. Figure out what data was stolen.

After speaking directly with the company, determine what data was stolen. Bank cards can be easily replaced; National Insurance numbers and HMRC details, not so much. You'll want to know what was compromised in the breach, so you can take the necessary steps to monitor or update that information.

3. Change passwords and turn on MFA.

After a breach, you'll want to quickly update to a new, strong password for the breached account and any account with the same login credentials. Additionally, if you see an option to log out all devices currently logged in to your account, do that.

While you're doing that, make sure you have multifactor authentication turned on in your account or privacy settings so that even if a hacker has your login, they can't access your account without your biometric data or a separate code.

4. Monitor your accounts.

Even after changing your passwords, you should keep a close eye on any accounts linked to the breach. Watch out for any account updates or password changes you didn't authorise. They may be a sign of identity theft. If your bank card number was stolen, pay attention to your bank and financial accounts and look for unusual activity, such as unexpected purchases.

5. Report it.

If you're not sure a company knows it's been breached or you've experienced fraud due to a breach, report it to relevant authorities like local law enforcement or the HMRC. They can provide guidance and next steps on how to protect your identity.

6. Be aware of phishing attempts.

Often, after data leaks, hackers use the information about you they stole to send you phishing e-mails or calls to trick you into giving away even more sensitive information. Be very wary of any e-mails you weren't expecting, especially those that request personal or financial information, and avoid clicking on any links or attachments.

7. Consider identity theft and data breach protection.

Consider identity theft protection after a breach, especially when highly sensitive data is stolen, like your HMRC login details. It's a time-consuming process to replace. In the meantime, criminals could be using it to impersonate you. Identity theft and data breach protection help monitor your credit or other accounts, protect your identity and notify you when your data appears on the dark web.

While companies are responsible for protecting customer information, breaches can and will still occur. By following the steps above, you can minimise a breach's impact on your life. Ultimately, we must all contribute to protecting our information in an increasingly risky digital world.

How to choose the best cybersecurity strategy for your business, ensuring you are prepared for both current and future threats?

Cybersecurity is evolving at a breakneck pace, and understanding the right tools is crucial for staying ahead of threats. In this e-book, you'll find a detailed comparison between Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR) technologies, both of which we recommend as the leading cybersecurity solutions.

- Is my current cybersecurity setup sufficient for emerging threats?
- How can I ensure complete visibility and quick threat response in my IT infrastructure?

To download this free e-book and see even more IT resources, all available for free, visit our e-book library at https://ergos.uk/resources/ebooks/.

CARTOON OF THE MONTH

"Here's what you're going to do. You're going to give those 3 million people their credit card numbers back and you're going to say you're sorry."

Early in his career, Mike Michalowicz was eager to announce to his team a new corporate vision for the year: a £10 million revenue goal. However, what he imagined would be one of his greatest visionary moments as a leader was one of his biggest mistakes.

After revealing the vision to his team, "it was total silence," Michalowicz explained to a room of business leaders at a recent industry conference. "A colleague came over to me and said, 'Mike, if we achieve £10 million in revenue, you get the bigger house. You get the new car. That's your vision. What about our vision?'". This was a transformative learning moment for Michalowicz, who committed himself to learning what it takes to be a GREAT leader.

Today, Michalowicz is the author of several books, including *Profit First, Get Different, The Pumpkin Plan* and other small business must-reads. He's an entrepreneur and speaker teaching other leaders how to build and retain unstoppable teams who care about the company's success as much as you do, so you'll be happier, grow faster and create an environment where everyone flourishes.

How To Build An Unstoppable Team

1. Most leaders tell their team what to do. Great leaders ask their team what they could do. In Maryland, US, Baltimore Museum of Art's most successful exhibit was curated by 17 museum guards. The idea came from a conversation between a curator and a guard around what the guard did day-to-day. He revealed how much he learned about the art from patrons and what interested them. Museum leaders quickly learned this wasn't unique to the one guard, and a group was assembled to create "Guarding the Art." Michalowicz explains that great leaders encourage ownership by asking, "What could we do?" rather than always telling their employees what to do.

2. Great leadership assembles and unifies. The 2010 movie *The King's Speech* depicts relationship between the King and his speech tutor working together to overcome King's stammer. This relationship is marked by trust and mutual respect, which Michalowicz says distinguishes great leadership in any circumstance.

3. Great leaders follow a FASO model. Michalowicz's research and experience in leadership culminate in a four-part model he calls "FASO." Leaders who want to be great can use FASO to assemble an unstoppable team.

- **F – "Fit."** When hiring a new team member, they must be an ideal fit for the organization, and the organization must be an ideal fit for them.
- **A – "Ability."** Great leaders look for people's raw potential. Do they have curiosity, desire and a thirst for the role? That's what great leaders hire and recruit for, not simply experience and innate ability.
- **S – "Safety."** Great leaders account for their team's physical, relational and financial safety. They ensure that people feel safe in how they are treated and where they work, they have a transparent financial culture and they educate their team on personal finances.
- **O – "Ownership."** "When we're forced to comply, we'll seek to defy," Michalowicz says. Great leaders encourage their team to personalise, gain intimate knowledge of and control aspects of their work.

Above all, Michalowicz says, "No one cares how you care; they care THAT you care." Show your team you care by working to incorporate these great leadership approaches in your organization.

ARE YOU USING THIS HELPFUL GOOGLE CALENDAR HACK?

It's a bit embarrassing when you log in to your computer at 9:00 a.m. only to realise you missed the all-team Zoom meeting at 8:30 a.m. Thankfully, Google Calendar offers a helpful hack: daily agendas. With this feature, you can send yourself a daily agenda first thing in the morning so you know everything planned for the day.

To set it up, log into your Google account and go to Settings. Find "Settings for my calendars" > "Other notifications" > "Daily agenda." The default is set to "None," so click on it and change it to "Email." Now you have a daily agenda automatically sent to your inbox before you even get out of bed!

CLIENT SPOTLIGHT:

INTERMEDIA BRAND MARKETING

"As a service provider to our publisher clients, we hold responsibility for the management and security of vast sums of customer data and therefore the integrity and performance of our IT infrastructure is pivotal to our ability to provide the highest possible level of client and customer service. ERGOS provide us with the technical confidence to protect our most valuable assets."

Would you like your company highlighted here? Contact your Account Director or call us at 020 3818 3411.