NEWSLETTER. OCTOBER 13, 2022

❤ #DoingSomethingGreat

THIS MONTH'S NEWS AND UPDATES:

Building successful brands by delivering great integrated customer experiences

DSG
DIGITAL SOLUTIONS GROUP

Digital Resilience

I am in the Bay Area, California, on a "workcation" meeting with technology partners. I decided to dedicate this newsletter to building Digital Resilience across your business ecosystem, as it is Cyber Security Month.

Since 2004, the President of the United States and Congress have declared October Cybersecurity Awareness Month, helping individuals protect themselves online as threats to technology and confidential data become more commonplace. The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) lead a collaborative effort between government and industry to raise cybersecurity awareness nationally and internationally.

As pioneers in Omni channel commerce in Africa, we paid some great "school fees" 😉 and experienced the phrase "Pioneers return with arrows in their back"😉

Fortunately, our resilient nature led to us surviving and thriving in the digital space.

We were first to market with e-commerce (1998) and mobile commerce (2000), so we learnt fast that internet fraud is a sad reality, and we need to build Digital Resilience in our business ecosystem.

Digitalmall.com was responsible for the first internet fraud arrest in South Africa to fight back against cybercrimes. As we gained popularity, every 4th transaction those days was a fraudulent attempt.

These early lessons in the evolution of our group led to us launching a dedicated company to cyber security in 2018, which we named Digital Resilience because we understood how important it is to be resilient when the threat landscape is ever-evolving and changing fast.

The goal of business should not just be to prevent unauthorised penetration, as it is almost too ambitious, but the focus should be to be resilient under attack.

The threat landscape is constantly evolving, so it's crucial to leverage Artificial Intelligence (AI) to analyse user behaviour and quickly detect threats.

Resilient companies quickly identify the unauthorised actor and limit the impact or activities of the hackers. By design, the business ecosystem architecture limits the potential for damage. For example, you can create business rules using a SOAR (security orchestration, automation and response) platform to improve the effectiveness of security operations by applying business rules in case of an attack that will make your security posture more effective.

We help companies build a SOC (Security Operations Centre) or offer it as a managed service. We use security orchestration to streamline people, processes and technology for greater effectiveness and efficiency. According to the latest Gartner SOAR market guide, "SOAR solutions are primarily adopted to create consistency in security processes and improve threat detection and response by providing context enrichment and improving downstream prioritisation."

I was privileged to attend McAfee Momentum, a global partner event in Napa, a few days ago. The highlight was a fireside chat between my friend Paul Towler and Leon Panetta, who has served in several different public office positions, including Secretary of Defense, CIA Director, White House Chief of Staff, Director of the Office of Management and Budget, and as a U.S. Representative from California.

It was an incredible discussion about leadership and challenges with the current security landscape and how cyberwarfare has taken centre stage. One of my key takeaways is that democracy has to be collaborative. Panetta emphasised human relationships and the need for public /private partnerships. He also mentioned the overall shortage of talent and awareness.

According to Cybersecurity Ventures, The number of unfilled cybersecurity jobs worldwide grew by 350% between 2013 and 2021, from 1 million to 3.5 million. The industry researcher also predicts that the same number of jobs will still be open in five years, which is a concern.

We need to invest in education to eliminate the “human firewall “ issues that are a considerable risk. We also need to create more cybersecurity professionals and provide technical training.

This challenge is an opportunity for Africa, especially because we have so many unemployed youths. We are currently running a 4 part series of webinars to educate corporates about the various critical success factors required for Digital Resilience.

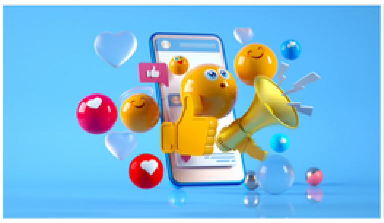
The first of the series was a webinar with LastPass focusing on passwords and passwordless future. Employee password practices remain the weakest link in a company's cyber security posture and maybe putting sensitive data at risk. We emphasised that while employees want to work efficiently from anywhere, businesses must ensure security controls are in place. 80% of cyber breaches are due to passwords; even worse, 85% involve a human element . Watch the recording here.

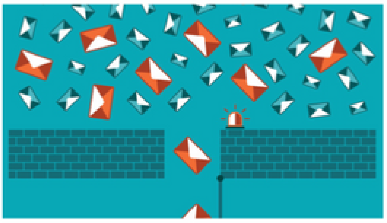
92% of people use the same password, or a variation is a risk… 51 % Rely on their memory to keep track of passwords. 65% Always or mostly still use the same password or variation, and 45% of survey respondents did not change their passwords which highlights why passwords are the leading cause of a breach.

I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

This past Tuesday, we ran a webinar with Beauceron Security which covered phishing "Do anti-phishing programs even work?" (watch here) and our focus is to create a positive security awareness culture within businesses and to mitigate the risk.

Phishing is a strategy by cyber criminals to obtain the personal or professional data of the victim. Users are tricked into providing confidential information, such as passwords and login credentials, through email, social media conversations or even banner ads.





We covered how to build an effective simulation program by providing access to different templates of varying difficulty and how to leverage the NIST Phish Scale framework.

It is tough to get to a "0 %" click rate on phishing, but the program can help reduce the number of clicks drastically, and we aim for a click rate target of more than 1% and less than 5%.

We use automated randomization of templates to reduce bias and make it easy for employees to report phishing and reward that behaviour.

Both platforms offer gamification and scores individual, business units and overall companies to ensure that we measure the effectiveness of the platforms.

At DSG, we take security very seriously and insist that employees keep their LastPass score above 80%, that Beauceron courses are used regularly, and phishing simulations.

It is amazing how many employees will click on an email offering a voucher irrespective of what they have been taught, so it is about repetition (aka mother of learning) and ongoing exercises that lead to lower risk.

hashtag#DoingSomethingGreat is making Digital Resilience a focus in your business.