WWW.HYPERGROWTH.GURU ISSUE 6

HyperGrowth ENTREPRENEUR

11 Powerful Customer
Testimonial Videos
Lemonlight

Mignon Francois:
A **$5** Decision That Changed Into **$10 Million**

"Forever" Decision
Getting Unstuck
Jeff Walker

GIVING BACK:
How You Can Change the World
Stu & Amy McLaren

He's on your doorstep!

Your Internet Security Approach Needs to Change... or he is going to get you

By Alfred Strauch

5 minute read

Editors note: Everyone needs to be concerned about security; however, business owners don't realize how unsecure their systems really are. Alfred makes a very strong case for how computing worldwide needs to change. And he provides the solution...new disruptive technology. Educate yourself. Protect yourself.

Using the internet for businesses is dangerous. Communication technologies are not safe.

Spies, criminals and malicious actors have always existed. Messages delivered by pigeons were intercepted. Letters were read and phone calls monitored. Malicious behaviors have not changed, but the methods and rewards have changed.

Malicious actors use social engineering, malware and automated processes to gather information. Big data combined with learning engines pinpoint targets and methods for intrusion. State actors, organized crime and corporate espionage understand how to use the weaknesses of our security infrastructure. The reward is money, competitive advantage or the competitor's destruction."

Worst Data Breaches and Cyber Attacks of 2021 So Far, by Rashmi Poddar, March 26, 2021
https://www.dailyhawker.com/tech/worst-data-breaches-and-cyber-attacks-of-2021-so-far/

February 8: One of the severe data breaches that took place in February 2021 compromised the health of thousands of people due to water contamination. The hackers attacked the computer system of **Florida's water facility,** which treats water for 15,000 people living near Tampa.

February 25: The hackers broke into **Oxford University's Biochemical Systems Lab**, which was studying COVID-19. Oxford University is considered one of the top biology labs in the world where some renowned professors were researching how COVID-19 can be encountered. All their initial findings and related data were hacked in the data breach. The leaked information included biochemical samples and other medicinal records researched by the university's researchers.

March 3: Cyber attackers have targeted not one but four security issues in **Microsoft Exchange Server email software**. The hackers used software bugs within the Exchange servers to get access to the email account of more than 30,000 firms all over the United States including local government, cities, towns and small businesses.

Why are these breaches occurring with greater frequency and ever greater losses?

The outrageous hacking statistics show that some of the cyber breaches are audacious, others outrageous, yet others simply stunning.

A few facts from the *https://hostingtribunal.com/blog/hacking-statistics/*

1. There is a hacker attack every 39 seconds. (Source: Security magazine)
2. Cybercrime is more profitable than the global illegal drug trade. (Source: Cybersecurity Ventures)
3. Hackers steal 75 records every second. (Source: Breach Level Index)
4. 66% of businesses attacked by hackers weren't confident they could recover (Source: Fortune)
5. 73% of black hat hackers said traditional firewall and antivirus security is irrelevant or obsolete.

Overall, organizations are spending 60% more than they spent three years ago, dealing with all kinds of insider threats. (Source: Observe IT) *https://techjury.net/blog/insider-threat-statistics/*

Why?

This leads us to an important question: Why are our IT/IoT systems vulnerable to attack? Why are users and the public complacent to threats of loss of identity, knowledge and resources? Why are businesses allowed to operate insecure systems?

The answer falls into several categories:

1. Investment in existing infrastructure.

A great deal of investment has been made in technology communication and technology infrastructure, but without security built into the core, issues persist. Experts predicted that worldwide global spending on information security should exceed $124 billion before the end of last year (2019) (Source: Tech Jury). Spending more money on the same strategies has minimal returns. Constant breaches suggest a new strategy is needed because the present solutions are not working.

2. Businesses manage security expectations to minimize liabilities.

Security professionals have limited options to stop breaches; therefore, they must deliver the best solutions possible with the budget provided and manage expectations accordingly. Businesses and users must demand change from the industry.

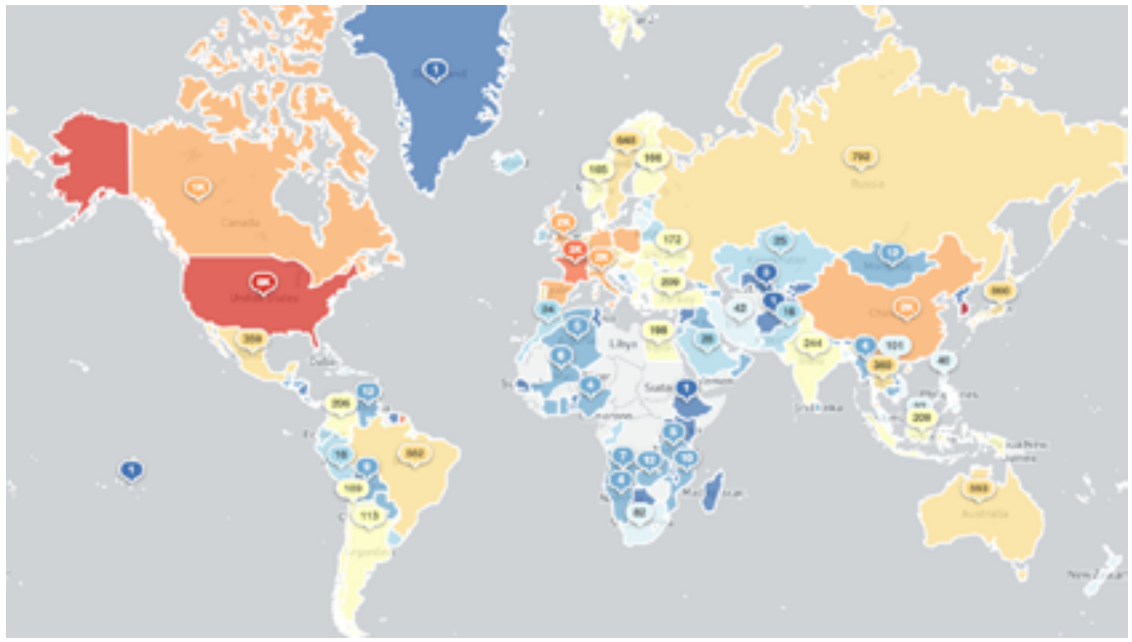
Solution and device providers say their devices are secure, yet they are being hacked. We must demand security and accountability from technology providers. The public must expect better from service providers, such as government, banks and businesses. People have the right to

know their information is safe and secure. Decisions related to information, sharing and ownership must be changed.

3. A lack of R&D investment and innovation in secure solutions and infrastructure persists.
An investment into a new architecture and protocol is required to stop the sinking ship from sinking. FUNDAMENTAL CHANGE IS NEEDED.

A new solution must also include a secure self-managed network with defined control processes for secure operation, management and support - a complete security solution.

Specific examples of secure failures include insecure printers and systems with default passwords. Printers are important IoT devices that are a prime vector for some attacks. Wireless communication whether in routers or printers are used as attack vectors into a network.



Exposed IPv IPP services by country (7th June 2020)

ShadowServer: Open IPP Report – Exposed Printer Devices on the Internet, JUNE 10, 2020
https://www.shadowserver.org/news/open-ipp-report-exposed-printer-devices-on-the-internet/

"Our IPP scans uncover around 80,000 open devices (printers) per day. This means these devices are exposed to outside parties.

Obviously, these counts only represent devices that are not firewalled and allow direct querying over the IPv4 Internet."
A firewall is minimal security for any implementation for the most basic implementations.

Consider a search from Shodan.com. Shodan is the world's first search engine for internet-connected devices. In one search, 6,268 servers and routers were found with default passwords, which means they are insecure.

Security is an issue, so what is the path forward?
To solve the technical security issues, we start with control. Who controls:

- Information
- Devices
- Communications

The General Data Protection Regulations (GDPR) correctly identifies the control of information and privacy as a human right. What does this mean to people when big tech companies build and control systems? How does this translate into systems, operations and users?

It is an oversimplification to say our core communication infrastructure is the problem, but it is a big part of the problem because it was not designed for secure communications.

> ***"Almost 30 years after its inception, it's time to fix the engine that both fuels the modern-day Internet and is the root cause of its most vexing security challenges." says Jeff Hussey in The Fundamental Flaw in TCP/IP: Connecting Everything,***

Billions of dollars have been spent building applications and solutions to fix fundamental TCP/IP problems; a system designed for connection efficiency not security while security remains a key issue.

"Dubbed Name:Wreck, the newly disclosed flaws are in four ubiquitous TCP/IP stacks, code that integrates network communication protocols to establish connections between devices and the internet. …. "It's a widespread problem; it's not just a problem for a specific kind of device," Costante says. "And it's not only cheap IoT devices. There's more and more evidence of how widespread this is. That's why we keep working to raise awareness." 100 Million More IoT Devices Are Exposed—And They Won't Be the Last, The Name: Wreck flaws in TCP/IP are the latest in a series of vulnerabilities with global implications. Lily Hay Newman, Wired 04.13.2021 12:01 AM *https://www.wired.com/story/namewreck-iot-vulnerabilities-tcpip-millions-devices/*

New Approach Required

A new approach is required built upon on new design principles such as the following:

Principles #1:

Build a communication model with security by design at its core.Effective security is a multi-faceted process including communications, devices and users. Security must include all these elements in its design.

Principles #2:

Real security is based on not trusting anyone or anything at any time. Relationships are based on trust. Trust is earned and tested. It is said a reputation takes years to build and can be lost in a flash. Security requires a continuous validation process to ensure all actions are valid.

Principles #3:

Ownership and Control are central to security operations. Who, what and why are questions central to the management of devices, information and operations within and between organizations. Controlling granularity is required for the protection of people, information and operations.

Principles #4:

Control requires accountability in ensuring responsibility is maintained. Accountability requires monitoring of users, devices and communications for malicious behavior. Malicious behavior comes in many forms, some intentional and some through ignorance.

Malicious behavior leads to consequences. Consequences require validation, reporting and restrictions of activities. Control therefore includes responsibility, Responsibility includes accountability. Accountability requires consequences.

The EU's General Data Protection Regulations (GDPR) illustrates the importance of data protection and fundamental principles for system design and implementation.

"The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her."

The building blocks of our technology infrastructure have been incremental. It is a jigsaw of parts, pushed together to solve problems and deliver services that work poorly.

The GDPR is a reflection of control of power, where the needs of people have been overlooked. Big tech, business, government and institutions have control while people are feeling powerless. Control is a real problem!

Some countries are implementing social credit systems to monitor and manage their population through the implementation of centrally controlled information systems. Some call this intrusive surveillance. People have little to no control over the operation of these systems or the information they gather.

IoT implementations lack some of the most basic IT security solutions. "The use of multiple layers of protection, including firewalls, authentication, security protocols and intrusion detection/intrusion prevention, is a long-established driving principle for enterprise security. In contrast, most IoT devices, especially sensors and low-cost devices, lack basic firewalls or security protocols, and often rely on little more than simple password authentication." Design World, How manufacturers can protect IoT products from cyberattacks, April 12, 2021 *https://www.designworldonline.com/how-*

manufacturers-can-protect-iot-products-from-cyberattacks/

How Important Is Iot To You And Your Business?

There are presently 200 billion IoT devices in the world Home cameras and surveillance systems, home automation, smart TVs, smart watches, phones and many more are consumer solutions.

Industrial solutions include robots, warehouse automation, HVAC systems, smart cars, self-driving tractors, medical devices and much more.

How does a lack of security impact IoT implementations?

Any quick web search will reveal doorbell cameras and other home surveillance system videos that have been hacked and posted to the internet. Hacks of cars, heart monitors, insulin pumps and many more have been demonstrated by white hat hackers and others.

IoT devices are changing how we live. Automation plays important roles in our lives whether you know it or not. Many of these devices are not secure. Are you willing to accept the risk intrusion or information theft? The call for more automation is increasing in volume, but our infrastructure is not ready.

How Safe Is Your Fish Tank?

"The attackers used that (a fish-tank thermometer – in the casino) to get a foothold in the network," Nicole Eagan, of security firm Darktrace, recounted. "They then found the high-roller database and then pulled that back across the network, out the thermostat, and up to the cloud."*(Gene Marks, Entrepreneur Magazine)*

The path forward is clear, we need an architecture and protocol to secure, operate, manage, monitor and support devices.

This means we need protected device mesh networks that do not rely on existing security solutions. In a protective device mesh, only peers (users or devices) can securely communicate. All other communications are blocked or rejected. Users and devices are governed by a "No Trust" policy. Mesh owners have complete control over information, devices, access and operations.

A new secure IoT architecture includes:

1. **Secure communications** so people and businesses can safely operate.
2. **Facilitate ownership** and control of devices and information so you can manage your own devices and information.
3. **Allow people and businesses to choose** who and how they share in operations so you can participate freely in the new digital world.
4. **Ownership includes responsibilities.** Participation includes accountability to your business, peers and related entities.
5. **Allow businesses to control** who, when and how information is shared to build viable mutually beneficial relationships.
6. **Restrict what entities see** when, why and how. Control includes the ability to grant, accept and restrict access related to operations.

Rethinking communications, relationships and how we operate in a new hybrid

economy (devices and digital) means the freedom for users and devices to work together and create beneficial relationships with security and safety. Our journey to freedom of operation has just begun. It starts with securing communications. It requires the implementation of fundamental rights such as the freedom to control data, operations and relationships.

There will always be malicious actors. The goal is to identify them and stop them before they can do any damage. More importantly, people need to expect safety and security from all systems; this requires new infrastructure solutions.

IoT manufacturers, industrial IoT users, or a heavy user of IoT solutions need to consider Smart Talk Beacon's secure protective mesh for security, operations, management and support.

If you want to see it in action, or you want to discuss these topics further, please contact me at alfred@smarttalkbeacon.com

Coach Gusty's Comments:

1. Talk to your security professionals and **get their feedback** in regards to the statements in this article.
2. How secure are you really? **Do an audit.**
3. Find Out more about this new technology.
4. Make security your **#1 issue**. Too many business owners think that if they are in the cloud, they are safe. That's not true.
5. **See it** in action – contact Alfred.

Alfred Strauch, President of Smart Talk Beacon Solutions Inc.
www.smarttalkbeacon.com