Aktuell Säkerhet

https://www.aktuellsakerhet.se/it-security-is-important-in-the-same-way-that-cleaning-office-toilets-is-necessary/
”IT Security is important in the same way that cleaning office toilets is necessary”
10/10/18

2018-10-10 | Linda Kante

Greg Ferro is Co-Founder of Packet Pushers Interactive LLC. An emerging media company covering the technology market from the perspective of an enterprise customer. We had a chat with him about the IT security landscape and it’s challanges.

What is Packet Pushers?

Packet Pushers is podcasts for IT Infrastructure professionals who want know more and make the most of your time in the car or on a plane. Our hosts are real engineers, talk nerdy and get the discussion into technology and not marketing. We’ve been doing it for ten years, we must be doing something right.

Today we have a 7 podcast channels focussed on data networking and cloud markets. Check us out on Apple Podcasts, Spotify or your favourite podcatcher by seraching for Packet Pushers.

You’ve said that IT security is overrated , can you develop on that?

Security is about protecting items of value to us. For example, we live in houses to keep the weather out but also to protect us from bad actors. We weaken the security

of solid walls by adding doors and windows we are making conscious decisions about balancing security against value of simple access, a nice view and fresh air. Some people have houses with valuable goods or high risk professions and will spend money to improve door locks, windows and may even go so far to install cameras and alarms.

IT Security is about protecting business operations for a cost. Its doesn't add value to the business by improving profits or sales so we want to cost to be low as possible. IT Security is important in the same way that cleaning office toilets is necessary but not important.

Companies Don't Fail Over IT Security

Surviving failure is normal for business. A bad deal, product problems, board collapse and management scandals are everyday events and companies continue on.

When we look at IT Security events over the last decade, how many companies were forced out of business ? Did they suffer long term loss of value ? Facebook has had a string of data breaches, Equifax, Heartland Payment Systems, British Airways – all major companies with huge security failures and zero impact.

Consider the Equifax hack in particular.

- A trusted technology company to manage highly sensitive personal data of credit checking that should have world class security functions.
- A key technology infrastructure for consumer financial transactions
- A series of security failures in 2016-2017 across multiple systems in multiple countries.
- Was breached by 9 month old published and well known vulnerability in their core business application
- IT security process shown to be laughably poor following audits
- Poor response to security incident with false statements, exaggerated claims, and even insider trading

While a few people lost their jobs, some with handsome packages, Equifax has suffered zero financial or business impact. They continue to operate credit services for profit.

If the business impact of IT security failure is so low, then we must focus on reducing the absolute cost. Here are some guidelines:

1. It must be cheap because the cost of failure is low.
2. It must be easy to manage like cleaning toilets
3. IT Security people need to understand they have limited value or importance and be realistic.

4. It must not impede the core business function and cause lost profits, lost productivity or lost opportunity. Security comes last because no profit means no need for security.
5. Companies must prepare for security failures as they do for any other failure (and maybe that means no preparation at all).

Simon Crumplin from Secrutiny said when you interviewed him that security needs more people and operations, not products. What is your opinion?

We need more people and less products. Why ? You need people to use the available tools and deliver business value. A threat intelligence feed performing inspection on an application firewall delivers no value unless it has ongoing configuration and analysis by an operator. As the apps change or new threats emerge it is the customers responsibility to observe and respond. Vendors and services are unable to deliver this customisation.

Companies like Secrutiny are showing companies that less products and more people focussed on common security tasks get better results. Simple activities such as patching,

Headcount Reduction Problems

Its been a boom period for security products over the last five years. Venture capital pumped 100s of millions into security startups to feed the executive fear cycle following the Snowden era five years ago. Sales teams are trained to sell on fear and uncertainty: upgrade to application firewalls for protection with new tools to detect attacks, replace your intrusion detection with cloud-based threat intelligence services.

The question “Are you secure? ” is an infinite selling opportunity that buyers cannot handle. Why ? Here are two reasons.

1. **Reducing Headcount.** Its the current fashion to reduce IT headcount to fund new purchases. IT budgets are not getting bigger so vendors have built products that “replace head count” and you can use the funds to buy more products. Of course, the IT team no longer has the time or skill to operate them to make the company secure.
2. **Lack of competency**. As headcount reduces, I see a colony collapse in technology competency. A small team often lacks the diversity and bandwidth to share, support and encourage each other. And the work commonly devolves into firefighting and job hopping instead of fulfilling creative and successful work.