THE
ENTERPRISERS
PROJECT

A community of CIOs discussing the future of business and IT

13 IT leaders confess their scary stories and deep, dark fears

13 IT leaders confess their scary stories and deep, dark fears

5 readers like this

By

Nano Serwich

on

Nano Serwich is Editor of The Enterprisers Project and Global Awareness Content Manager at Red Hat.
» More about me

October 25, 2016

reddit

googleplus

Today's IT leaders are facing a world of unknowns and underlying fears on a daily basis - from the ransomware that could take down their organizations, to the emergence of new digital disruptors that could render their business obsolete, to the absence of quality IT talent they need to stay ahead of these and other threats. Although scary, it is comforting to know that you are not alone.

We asked 13 IT leaders to share their stories of unexpected or frightening events in their career, or the threats on the horizon making them nervous for the future of IT. Read on for their tales from the IT crypt.

$2M for unindexed unknowns

"A Fortune 500 company had an estimated 500,000+ boxes of business records stored with both physical records management vendors and at the company's locations throughout the United States. They pay $2 million per year in box storage alone, but they have no idea what is in the hardcopy business records; the boxes are the 'unindexed unknowns.' There is likely a significant risk for PII and PCI given the industry the organization is in. Presently, the company does not have the internal bandwidth nor financial appetite to locate, index, and digitize all of the paper records, thus leaving them extremely vulnerable to a breach."

Farid Vij, Director, Information Governance and Analytics, ZL Technologies

No access to backed-up data

Related Topics

What digital transformation means at Royal Caribbean Cruises
Submitted By Minda Zetlin
October 25, 2016

In an IDC survey, two-thirds of CEOs said they intended to focus on digital transformation this year. Yet most companies fail to create the transformation they're hoping for.

Read Article
SAS CIO: Why CIOs should attend analytics training with their IT teams
Submitted By Keith Collins
October 24, 2016

I see my approach to skill development as a journey, and important to that journey is creating more people who have a deep understanding of the art of the possible. That's why I wanted to be in the classroom taking the course with my team.

Read Article
HBR article: You may not need big data after all

"We'd always been proud of the fact that we had our data backed up, as so many businesses fail to do this and leave themselves vulnerable. But when we checked our backup data a few months ago, we realized that we couldn't access it and that even if we could, we were missing important files. We learned our lesson, and now we make sure to have data recovery drills quite regularly, but the fact that we would have been left without all of our data in the event of an accident was very scary indeed!"

Max Robinson, Ace Work Gear

A stranger in your email

"A new scary form of hacking that is on the rise, and totally out of the control of the IT department, is social hacking or social engineering. Hackers take advantage of human nature and use that to try and gain access to restricted information without the proper permission. For example, a hospital employee may receive an email from someone claiming to be the CFO, with an email that has one letter off in said CFO's name, urgently requesting an invoice containing sensitive information. In a rush, the employee may not realize that one letter is different in the 'CFO' email address, promptly sends the info, and the hacker is in. Since it is difficult for employees to say no to authority figures or familiar contacts, they're more prone to give out sensitive information. What is scary is that people don't take the time to check or think about what is being asked, and the hackers are counting on this."

Scott Youngs, CIO, Key Information Systems

Hidden skeletons in IoT

"The scariest things in IT are the 'hidden skeletons' that may pop up in the coming months when it comes to mobile and IoT applications (especially for connected cars and connected medical devices). Most organizations are not aware and prepared for attacks at the mobile app level, which has become the weakest link. Attacks are already happening at the mobile level in banking, retail, and other sectors, but nothing has been publicized. Organizations that are getting complacent are in for a rude awakening. For IoT apps, some of the leading edge companies are doing a good job securing their infrastructure, but according to results from various surveys, they are way behind the deployment roll-out. And, hackers are lurking to launch

Submitted By: Nano Serwich
October 23, 2016

With all of the hype about big data, companies are signing up without taking inventory to see if the capability already exists within their enterprise.

Read Article

Recent Tweets

Tweets by @4enterprisers | Follow @4Enterprisers that major attack that could cause havoc. Watch out for these skeletons that could jump out at any time!"

Mandeep Khera, CMO, Arxan Technologies

Corrupted data

"In a past life, we had a scare where one of the production database backups stopped working and no one knew about it. Of course, we had a production outage and the data was corrupted – we then tried to recover from the last good backup, which was over two weeks old. Ouch! Luckily, we had taken the database snapshot the day before, so we restored using that data. But it was quite a nightmare – we ended up losing a little bit of data, a lot of sleep, and even some hair in the recovery process – but we learned to double-check our backup processes often and build strong, reliable alerting."

Rajeev Jaswal, Chief Information Officer, Rapid7

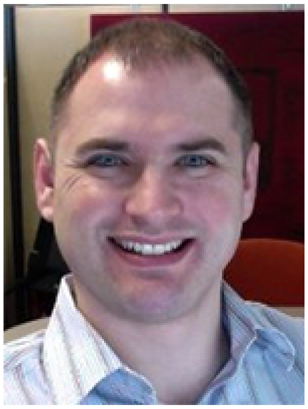
Beware of ransomware

"As a former cyber security advisor for the regulator of our nation's power grid, I have seen a lot of scary experiences in my career. Currently, running a cyber security education company, we have heard a lot of challenges with ransomware. One, in particular, affected organizations we spoke with that operate the nation's power grid. A machine was ransomwared and demanded a $10,000 payment in Bitcoin. The organization paid, and then executives quickly realized a plan needed to be put in place in case this happened again. Most organizations are not prepared for events like this that will only get worse, and what we see is usually a reactive response instead of proactive thinking."

Nick Santora, Chief Executive Officer, Curricula

The phones are dead

"In a previous role, I had some hardware completely stop working on our primary phone system. We had a four-hour SLA for hardware replacement with our vendor, but they ended up having some logistical problems and couldn't provide the new hardware for nearly two full days. Imagine a sales department not having working phones for multiple days. Thankfully we had backups, but they had to be restored to hardware that wasn't readily available. I had to improvise and created a virtual machine that mimicked the hardware, had a buddy strip the bootup code, which did a hardware check and restored the backup in a virtual system. It's worth noting here that this was something TAC said wasn't possible or supported, but desperate times call for desperate measures. It worked, and we had phones for those three days. Even if you have everything ready for when things go wrong, you can still end up in a rocky place."



Derek Heintz, Director of IT Infrastructure at Rapid7

Part Two: Return of the ransomware

"Before I started my entrepreneurial journey, I sold security software for a Fortune 50 tech company. Ransomware is becoming more prevalent, and hackers are attacking companies that are not using AI technology. Just like Pandora uses AI to predict what music you will like, this technology can detect possible ransomware threats. I witnessed a hospital in California be shut down because of ransomware. They paid $2 million in bitcoins to have their network back. This is enough to scare every small business owner."

Gene Caballero, Co-Founder, GreenPal

Trick or treat in the cloud

"It's nearing Hallows' Eve, and while I prepare to carve pumpkins and deal out candy to little ghosts and goblins, I can't help but think of the scary environment that today's CISOs operate in. Whispers and chatters are growing louder within the Darknet, and we must anticipate and prepare for crypto war attacks that become more vicious by the day. There are no treats when these villains come calling – only demands for ransom that leave a bitter taste in our mouths. But in designing systems that have the ability to reset without negotiation, we can guard against their tricks and protect our business and our brands."

Lakshmi Hanspal, Chief Security Officer, SAP Ariba

Revenge of the disgruntled former employee

“Next time you have to let an employee go – you can take his laptop, you can take his badge, but you cannot take his personal devices, and you cannot take his thoughts. This scary story starts with one of our customers with an embittered employee that after being let go, connected to the company network through the wireless since he knew the password to it (shared key). From there he downloaded ransomware on one of the servers, and the mess began. If you are not controlling the access to your network, you are not in control.”

Ofer Amitai, CEO & Co-Founder, Portnox

Don't be scared of risk-taking

"In a large enterprise environment, there can be hundreds, if not thousands, of changes to infrastructure, applications, or platforms each week. Each change presents a risk, but we cannot let it scare us from moving forward. Changes do not have to become nightmares. Every day we must deliver to the best of our abilities and not focus on the ghosts of our mistakes."

Cassie Crossley, Director I.T., Schneider Electric

Nowhere to hide from breaches

"A trend that frightens me in IT right now is the growing notion that breaches are going to happen and are therefore unavoidable; almost even acceptable. This way of thinking is taking the focus away from preventing threats and almost glorifies the attackers for their ingenuity in the aftermath. It's a self-fulfilling prophecy. Accepting breaches as a cost of doing business is essentially inviting ransomware over for dinner."

Joe Dahlquist, VP Product Management, ThreatSTOP

Doomed to repeat mistakes

“In my many years of experience helping some of the largest organizations in the world roll out effective application security programs utilizing SAST the scariest trend I have seen is that application security takes a back seat to new features being released to the market or a hard release date. Application security is important but only when it is convenient and does not interfere with business drivers. Companies try to solve the application security problem with products and neglect to define and implement the process with the associated application security products. The fundamental misconception about application security is that it is not about just 'scanning code' but rather remediating real issues and educating developers how not to make the same mistakes over and over again.”

Matt Rose, Global Director Application Security Strategy, Checkmarx

Related content

4 IT leaders discuss IT's role in the Internet of Things

Advice to prevent insider security threats

Survey finds companies are still not prepared for major security incidents

Tags:

- Security

reddit

googleplus

Post Comment

Comments 0 | Add yours Below

Comment Now

Your name *

E-mail *

The content of this field is kept private and will not be shown publicly.

Homepage

Comment *

□ Notify me when new comments are posted

□ Accept the Terms of Use to continue. You are licensing your contribution(s) as CC-BY-SA. *

By submitting this form, you accept the Mollom privacy policy.

Save

About This Site

The Enterprisers Project is an online publication and community focused on connecting CIOs and senior IT leaders with the "who, what, and how" of IT-driven business innovation.

The opinions expressed on this website are those of each author, not of the author's employer or of Red Hat. The Enterprisers Project aspires to publish all content under a Creative Commons license but may not be able to do so in all cases. You are responsible for ensuring that you have the necessary permission to reuse any work on this site. Red Hat and the Shadowman logo are trademarks of Red Hat, Inc., registered in the United States and other countries.

A note on advertising: The Enterprisers Project does not sell advertising on the site or in any of its newsletters.

Connect

Follow us @4Enterprisers on Twitter

Like The Enterprisers Project on Facebook

Watch us at The Enterprisers Project

Join us on Google+

Connect with us on Linkedin

RSS Feed

Let us bring the conversation to you

Enter your email

Twitter
RSS
Log in
Register

Privacy Statement | Terms of use | Contact