IT ONDEMAND
it-on-demand.com

THE TECHNOLOGY TIMES NEWSLETTER

Creating a High Reliability Organization for Your Business

Experts agree: technology alone will not protect your company from cyber threats. In the majority of breaches, human error plays a factor, regardless of how sophisticated the technology may be. However, when paired with up-to-date tools, a company that respects and follows safe cyber practices can drastically improve its security.

The difficulty lies in creating that culture of cybersecurity. In recent years the US military –which faces tens of millions of cyber threats every day – has addressed this very problem by adopting a High Reliability Organization (HRO) methodology. The concept of an HRO came from industries in which even a small mistake could have disastrous results, such as air traffic control and nuclear power plants. Today, businesses of any type can learn valuable security lessons from HRO practices. These principles include being aware of your vulnerabilities, consistently maintaining high operational standards, being vigilant, and having clear methods of accountability.

HRO's abide by six core values: Integrity, Depth of Knowledge (i.e. giving your employees an understanding of the bigger picture of how and why these systems work), Procedural Compliance (and inspecting that compliance periodically), Forceful Backup (e.g. two-step authentication policies), A Questioning Attitude (i.e. encouraging employees of all levels to speak up when something seems wrong), and Formality in Communication. If and when incidents occur, it is almost definitely due to one of these principles being ignored. However, each can and should be adjusted to best fit a company's needs.

These principles create a solid foundation from which to build a better-protected business. Be firm and consistent with your security policies, and use inevitable mistakes as an opportunity for everyone to learn. Ultimately, as a CEO engages with and values cybersecurity, a company culture of High Reliability will begin to form. **For assistance on your security as well as your written procedures, please contact us at (212)235-0260.**

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"
Howard Globus,
IT On Demand

Providing Excellent Support to the New York City Area

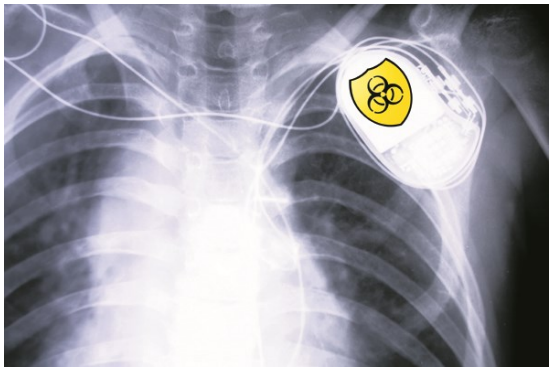
Inside Our October Newsletter...

Is Your Pacemaker a Threat?: Cyber Attack Warning from the FDA

Over the summer, the FDA released a safety warning regarding an infusion pump typically used in hospitals. The pump, made by Hospira, was determined to be vulnerable to cyber attacks; the FDA recommended that hospitals replace them with alternative pumps to avoid endangering patients. The notice is the first of its kind, and comes at the heels of new guidelines also issued by the FDA requiring better security standards from manufacturers for their devices.

While it may seem like science fiction, the fact is that hackers can now access a multitude of medical gadgets, including insulin pumps, cochlear implants, and pacemakers. The latest technology in these devices allows data to be sent and received via wireless internet, leaving them – and their users – at risk.

Thus far, no one has been harmed by such a breach, but there have been incidents. Cybersecurity firm TrapX released a report this year detailing three attacks in which equipment like an x-ray system and a blood gas analyzer were infected with ransomware and other types of malware. And the danger of hacking medical devices is two-fold: not only can the devices be tampered with remotely, potentially harming a patient, but personal data can be collected, too, which is far more desirable to hackers than financial information.



With advances in both wifi-capable technology and the ability to infiltrate said technology, the time has come for advances in our cybersecurity as well. As the FDA continues to investigate the safety of these devices, expect to see new warnings and updated security guidelines in the future.

FREE Report: The Business Owners' Guide To IT Support Services And Fees

You will learn:

- The 3 most common ways IT services companies charge for their services, and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

Claim Your FREE Copy Today at
www.it-on-demand.com/itbuyersguide/

Shiny New Gadget Of The Month:

THE AMAZON ECHO: LIKE SIRI FOR YOUR HOME

It's not Rosie the Robot, but your first voice request to Amazon's new Echo moves you one step closer to living like the Jetsons… Think of it as a plugged-in version of Apple's Siri or Microsoft's Cortana.

This "smart" speaker in a 9¼ x 3¼-inch cylinder can order products, turn off lights, set a timer, look up and give you sports scores, read you a book from Audible and more.

You might even get it to tell you terrible jokes…

It won't replace a high-end stereo, but its sound quality compares with any Bluetooth speaker, and it can fill a good-sized room in your home.

Bottom line: Echo offers hands-free, at-home audio access to just about anything on the web, with better sound than a smartphone or tablet.

All in all, it can make your life easier. And maybe just a little more fun.

Carjacking via Hacking: The Big Gap in Car Safety

Every day, it seems, we integrate WiFi technology into more and more aspects of our lives. Home appliances, medical devices, and cars are now all made with communication capabilities. Unfortunately, these advances have left our privacy – and our safety – in jeopardy. This vulnerability is especially true in the latest cars on the market. For more than twenty years, automakers have been putting computers in vehicles while failing to anticipate and protect against the weaknesses such features might entail.

These security concerns are getting plenty of attention, too. Car company Tesla made headlines when researchers discovered a way to "hotwire" a Tesla car with a laptop. The latest season of *Scandal* featured a plotline in which a car was hacked, making an assassination look like an accident. Professional hackers Charlie Miller and Chris Valasek have created multiple carjacking demonstrations; one, in which a car was remotely brought to a stop on the highway, led Fiat Chrysler Automobiles to recall over a million vehicles.

As consumers become more aware of the danger in these vehicles, legislators are putting the manufacturers under scrutiny. In September 2015, leading automakers were asked by members of the Senate to provide information on the safeguards they have protecting their onboard systems from attacks.

Still, achieving more secure vehicles will be a long process. In the meantime, carefully research before buying a new car; ask about the wireless features available and talk about whether remote shut down is enabled. Some makes and models are more at risk than others, and the information is available online. By choosing secure cars, consumers can send a clear message to automakers about the necessity of closing their security gaps.

Put a Hacker on the Payroll? The Burgeoning Legitimacy of the Hacker Industry

For decades the term "hacker" has been associated with being a menace, and often a criminal one. Even today, the general public tends to assume hacking to be an unethical activity at best. But not only is that not necessarily the case, the fact is business owners, even those with small businesses, can benefit by putting hackers to work for them.

Though the business of hacking certainly still has its unsavory side, today many hackers have found a market making themselves available for perfectly legal and upstanding services. The terms "black hat" and "white hat" are used to denote the difference; malicious, criminal hackers fall under the black hat label, while white hat hackers choose to use their talents ethically.

As the field of cybersecurity explodes, hackers are highly sought after for their ability to anticipate security weaknesses and develop better barriers against them. Rideshare company Uber, for example, recently hired hackers to help develop defenses of its self-driving car technology, according to a report from the Wall Street Journal. So-called "hackers for hire" address a variety of needs on-demand as well, from hacking into locked email accounts to investigating online predators.

Amidst these reports and promises of useful, unique services, business owners should still proceed carefully when considering hiring a hacker. Be sure to research potential vendors thoroughly and consult with trusted IT professionals to determine the risks and benefits. Used wisely, a hacker can be a valuable resource to you and your company. Please contact us with any questions you may have at **(212)235-0260**.

On A Side Note... Could Your Laptop Battery Revolutionize The Way We Drive?

If you like hot cars and green tech, you may have started hankering for a Tesla as far back as 2008…

Yet, aside from cool looks and speed, did you know the simple design edge that's putting Tesla in the spotlight?

Other car builders, like Nissan, GM and even Mercedes, have electric cars on the road. But they all use costly, high-tech lithium ion batteries.

Tesla, on the other hand, simply uses the type of batteries you have in your laptop – thousands of them…

With over a billion of these cells made every year, their design and pricing is driven by the same fierce competition that drives the consumer market.

And if Tesla Motors can put a car on the road with enough battery life, they may just revolutionize the way we drive – like Henry Ford's Model T did over a century ago.