An eBook from
Mat Dirjish, Executive Editor

sensors ONLINE
Your Technical Resource for
Sensing Communications & Control

SECURITY REPORT, RESEARCH & ROUNDTABLE

Security Concerns Today and what to Expect in the Expanding IoT

INTRO & TOP FINDINGS

SECURITY EVOLUTION

SECURITY PRESENT

WHAT THE WARNING STUDIES SAY NOW

ON THE OTHER HAND

SECURITY ROUNDTABLE

WHAT TO DO AND WHAT TO EXPECT

PREDICTIONS, MUSINGS, AND RAMIFICATIONS

THE PENULTIMATE WORD

COMPANY PROFILES

CONTACT

REFERENCES

Intro & Top Findings

Each year the tech community embraces several hot buzzwords, which obviously pertain to the "next big thing", another buzzword that has been worn slimmer than the frets on a blues-player's guitar. For the past several years, the Internet of Things (IoT) has been the big thing, heralded and lauded with terra bytes of media on a minute-to-minute basis. Claims ranging from it's coming, it's here, it's slow, it's fast, it's going, damn it I missed it, to what this author says: the IoT is networking.

The IoT is networking a whole bunch of stuff over the internet, something that has been going on for at least three decades now. The difference between now and then, is now there are millions more devices networked over the web with, allegedly, trillions more to come. And with this mass proliferation of networked devices comes a massive amount of opportunity.

Sensor makers are sitting in the sweet spot as just about every new device hooking up with the internet requires sensors, in many cases, a lot of sensors. Wireless and power-source designers also have a great stake in IoT designs as nearly all remote control is delegated to smartphones, which require highly efficient, clean, and long lasting operating power. Embedded system designers will also profit as all of the networking topologies and devices will require interfaces and data collection/processing hardware. And software programmers have it made since they will be providing the code to make all this interconnectivity and networking possible as well as creating the apps for data acquisition and analysis.

In addition to engineers, designers, EOEMS, and programmers, the IoT offers great opportunity for another group of very talented people, though inversely gifted. All those networked devices, interfaces, embedded systems, wireless phones, and applications provide a veritable wonderland of opportunity for hackers, phishers, identity thieves, and many other scammers. Yes, every playground has it's bullies and muggers, and every playground needs its heroes.

Software developers are sitting in both an enviable and frustrating position. Enviable in that, as mentioned earlier, the IoT runs on various types of software, of which there is always demand. Much profit is possible. The frustrating component is keeping all of these devices secure and safe from the bullies and muggers on the playground.

In the analog world of long ago, if you beat up the bully once or put the mugger in jail, that was all that was necessary. Other bullies and muggers got the message and stayed away. But when you have a near-infinite playing field with millions of independent bullies working simultaneously, eliminating a couple hundred would not even be noticed by anyone, and they would soon be replaced by more than the number eliminated.

- Sensors, Sensor Systems and IoT Devices are targets for cyber-attacks.
- Over 50% of financial institutions have been subject to cyber-attacks – security software developers need to take this threat seriously.
- Pressure to get IoT devices on the market makes security an afterthought – sensor makers, OEMs and embedded system developers need to make security a priority throughout the design process.
- Smart homes are highly insecure due to users' failure to follow best practices – device makers need to educate consumers, make security products easier to install.
- Companies are failing to take crucial steps as part of the preparedness process – embedded systems need to be made more secure, yet simpler and more cost effective, in particular using Open Source Platforms and Encryption are a necessity. Also, Security Standards are needed and should be followed for protecting Sensor Systems.
- 66% of consumers feel emerging IoT devices will be hacked – IoT device makers need to educate consumers, quell negative view of connected devices.
- 100% of reported vulnerabilities in the IoT are avoidable – OEMS, parts makers, and security pros can effectively secure devices.
- Attacks from the Cloud or Poorly Secured Wireless Networks are a big concerns that Engineers should anticipate during the Design Process.
- 90% of employees bypass security – employee behavior needs to be modified, implications of actions need addressing.
- Consumers suffer from security overload – education is the key, followed by simplification and security imperative.
- Engineers need skill development to address the evolving threat landscape. Reading articles and going to shows are ways to achieve this.

An eBook from
Mat Dirjish, Executive Editor

sensors ONLINE
Your Technical Resource for
Sensing Communications & Control

INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

Intro & Top Findings (continued)

Security is probably the biggest buzzword at this point and the biggest concern surrounding new technological advancements. Anything connected to the web is vulnerable to attack. Software designers play a game that never ends. First, assuming the product deadline is not pressing, they create what they believe is a secure application. Second, the product hits the market and a clever villain figures out how to hack into the software. Third, and perhaps with a software or firmware update/fix, the software designer corrects the problem. Then again a hacker finds a way in, and the cycle continues.

Compared to hardware makers, software folks have it rough. These days, there's no real profit in stealing hardware unless it's useable right away and can possibly be fenced for a profit. A car or other large vehicle comes to mind. However, since there is video surveillance everywhere, vehicle theft is risky. Even if successful, a complete vehicle is easily traced, limiting the fence off to chop shops.

Hardware, if necessary is far easier to secure than data. Lock your hardware in a rad-hard container capable of withstanding a 100 Giga-ton nuclear blast and arc-weld it to the face of the earth and it's not going anywhere. Obviously, most hardware is not valuable enough to secure so well.

Software, as mentioned earlier, offers ongoing challenges for the villains, challenges more often easily overcome than not. It's an ongoing battle that will not end. It can't be won; the threats can only be kept at bay, they will never stop because you can't stop all the bullies and muggers.

The purpose of this report is to look at some of the key security issues the industry is facing now in terms of what problems exist and possible solutions. It also looks at what's being done, what's not being done, and what should and could be done.

Though somewhat lengthy, the report contains just a small sample of the coverage given to security, IoT, and embedded topics you will find available at Sensors Expo West 2017. There you will hear and meet the experts who will tell you face to face what the deal is with security. Also, at the end of this report are links to 2016's security surveys, studies, findings, and predictions. Best part is you won't need a username or password to proceed.

An eBook from
Mat Dirjish, Executive Editor

sensors ONLINE
Your Technical Resource for
Sensing Communications & Control

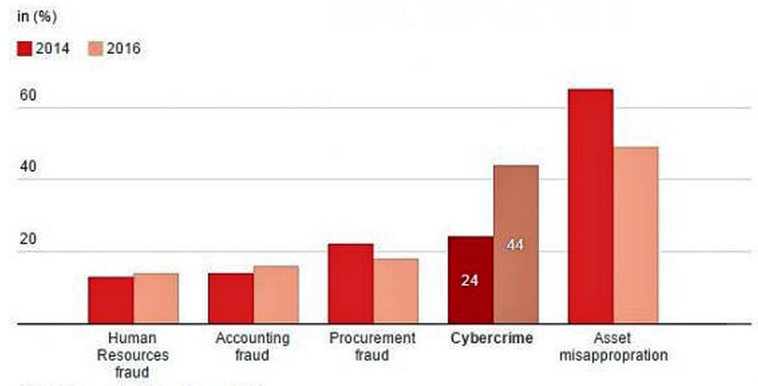
INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

Security Evolution

Since the early days when personal computing was just starting to pique the interest of the masses and the internet was a handful of computers connected over plain-old-telephone-service (POTS) copper wire, security was a concern reserved only for the connected few. In most cases, a username and password would do.

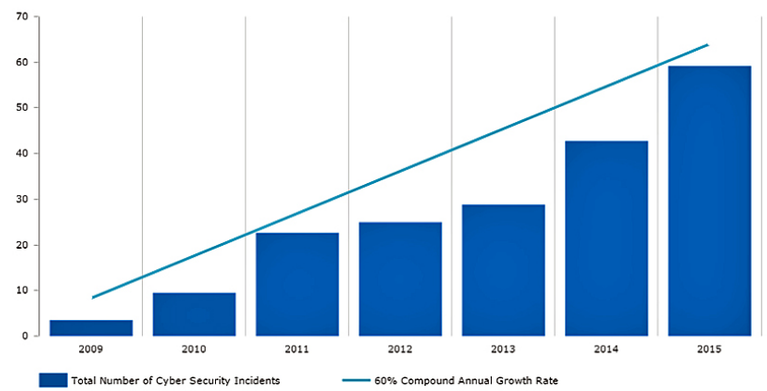
As the hardware became faster, software more sophisticated, and networking expanding exponentially, the hackers and thieves became many and more sophisticated. Anti-virus software became a necessity for even the simplest connections and networks. As email became more accessible and viable for commercial and governmental use, complex encryption and algorithms came on the scene. **And as each new security topology emerged, so did a new wave of invaders, more sophisticated than the last.**

Cybercrime climbs to 2nd most reported fraud in 2016



In 2016, cybercrime took about a 20% leap from 2014, making it the second highest form of fraud by not that much of a margin over asset misappropriation.

Cybercrime Keeps Climbing, Despite Increased Spending on Security Technology and Services



Source: PwC Global State of Information Security Survey 2015 & 2016

According to a Source PwC survey 2015/2016, cybercrime is on a steady and, unfortunately, healthy rise. The trend is expected to continue as the IoT also expands.

An eBook from
Mat Dirjish, Executive Editor

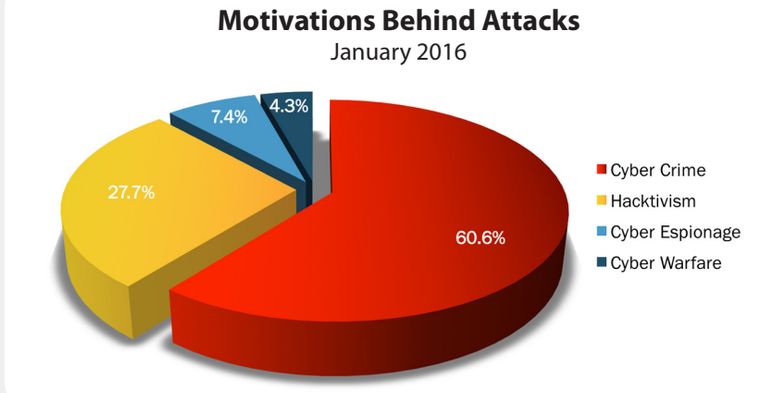
sensors ONLINE
Your Technical Resource for Sensing Communications & Control

INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

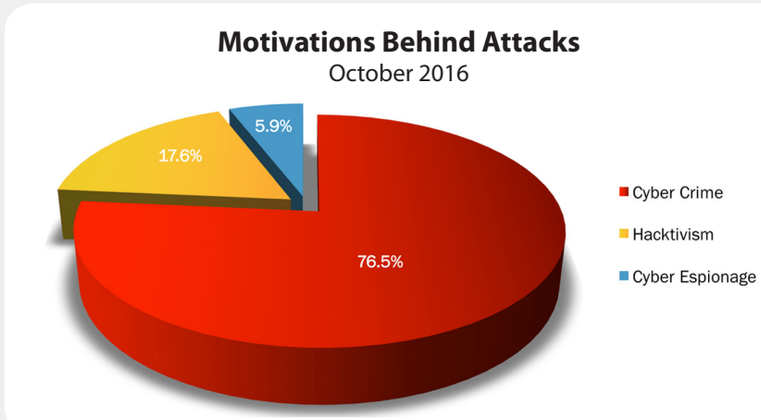
Security Present

Rather than go on ad infinitum about all that's occurred in between, fast forward to now – 2017. Here we are at a point in time where billions of devices interface to the internet with trillions more forecasted for the near future. Each one of those devices, to greater or lesser degrees, pose a risk to their users. If it's on the web, it's fair game for hackers.

In some cases, devices and connections are the target of harmless, yet disconcerting, practical jokes. But more often than not attacks are with malicious intent, i.e., theft (monetary and identity), vandalism, chaos, havoc, etc. If you view the internet as a large house and each connected device a door or window, it's obvious that the more doors and windows your house has, the more opportunities available for unauthorized entry.



Motivations for cyberattacks between January 2016 and October 2016 show a near 16% increase in cybercrime (identity theft, monetary theft, etc.) with a 10% decrease in hacktivism (snooping, privacy breaches, etc.) and a 1% decrease in espionage. The reason for these changes may be cybercrime is more profitable, hence, the significant increase. Though changes are small, hacktivism and espionage are an ever-present threat as well as the potential for a flare up in cyber warfare events. Again, it's important to note that the overall numbers for each category are significantly large. (Graphs and research from http://www.hackmageddon.com)



An eBook from
Mat Dirjish, Executive Editor

sensors ONLINE
Your Technical Resource for Sensing Communications & Control

INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

What The Warning Studies Say Now

Most of the emerging security studies focus on negative scenarios, so much so one may be led to believe the future is pretty bleak. Then there are a rare few that say there's not much to worry about, hope and help are on the way. But for starts, let's look at the "sayers of gloom."

Attacks on financial institutions are fairly common, reports on these show up regularly in mainstream news channels. **According to a recent MetricStream Research survey, two-thirds of financial institutions participating in the survey reported they had experienced a cyberattack in the past year.** Respondents were C-level information security professionals associated with 60 global financial services firms of various sizes and segments. These include banking, insurance, asset management, diversified financials, investment services, and foreign exchange services.

On the consumer/renter/home-owner front, the non-profit prpl Foundation did a global study on the use of smart devices in a domestic setting. The report, titled "The prpl Foundation Smart Home Security Report", cites three key issues:

1) The smart home is here and device adoption in certain cases has reached a tipping point
2) The smart home is highly insecure due to users' failure to follow best practices
3) And consumers prefer security to usability, and they're prepared to take more responsibility if it means living in a safer home.

Researchers at Context Information Security focus on somewhat of a "no brainer" when it comes to security. They find that the mad dash to get IoT devices on the market have their makers taking shortcuts when it comes to securing their devices. **Security is an afterthought, if at all in some cases.** The researchers point to numerous stories involving successful hacks into connected devices from lightbulbs and children's toys to surveillance systems, conference phones, and connected cars. They claim that this demonstrates that vendors are not taking cyber threats seriously. It's not just new products or naïve vendors: big companies are making the same mistakes.

They say failure to prepare is preparation to fail, and it's always amazing how often "they," whoever "they" may be, are correct in their observations. "They" in this case is the Experian Data Breach Resolution. Its annual Ponemon study on data breaches finds companies lack confidence and are failing to take crucial steps as part of the preparedness process. Companies must realize that planning is not the same as being prepared.

According to a report from KPMG Cyber, the "Consumer Loss Barometer", nearly a third of consumers limit their use of IoT devices due to security concerns, and 61 percent said they would use more devices if they had greater confidence in their security. Three-fourths of millennials said that they would use more IoT devices if they were more confident in their security. Overall, 66 percent of consumers feel emerging IoT devices will be hacked.

An eBook from
Mat Dirjish, Executive Editor

sensors ONLINE
Your Technical Resource for Sensing Communications & Control

INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

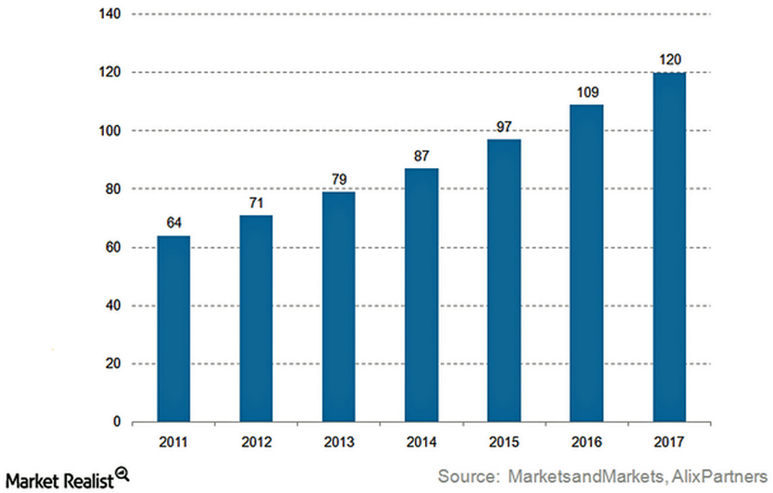
On The Other Hand

There are studies that reveal the underside of the aforementioned examples. They indicate security weaknesses and general bad practices. Of course, there are not as many positives as negatives.

For example, a recent study by the Online Trust Alliance (OTA) claims **"100% of reported vulnerabilities in the IoT are avoidable."** The OTA claims that, if device manufacturers applied the security principles outlined in the OTA IoT Trust Framework, that susceptibilities in products developed after November 2015 would have never occurred. This echoes back to the Context Information Security study that found security practices are neglected by device makers in favor of a speedier time to market.

In the play Julius Caesar, Shakespeare wrote, "the fault is not in our stars but in ourselves" and such can be derived from a CEB study that found **90% of employees bypass security.** Companies are on top of things, increasing security tech investments; however, in many cases their employees pose bigger threats than the hackers. This is comparable to the person who goes to the doctor with an ailment, the doctor diagnoses the ailment, prescribes medication, and the patient doesn't take the medicine.

Similarly, a Symantec survey reveals that consumers suffer from security overload. Accordingly, the survey found **79% of consumers know they must protect their information online, while 44% felt overwhelmed by the sheer amount of data they are responsible for.** Once again, the fault lies with the users, not the tools.



According to a MarketasandMarkets report, opportunities for innovation, growth, and profit for cybersecurity professions on the rise. In 2017 the market is expected to garner about $120 billion, no small figure.

An eBook from
Mat Dirjish, Executive Editor

sensors ONLINE
Your Technical Resource for
Sensing Communications & Control

INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

SECURITY ROUNDTABLE:

What The Pros Know

Vaughn Emery
CEO & President
CENTRI Technology

Alan Grau
President and Co-Founder
Icon Labs

Mille Gandelsman
CTO and Co-Founder
Indegy

Jon Stark
CEO
Peratech Holdco Limited

Larry Stefonic
Founder
wolfSSL

Scott Keller
President
Signal Fire Telemetry

Research studies and surveys are often good indicators of certain conditions and behaviors. They either make or can be used to make predictions, or, better put, somewhat educated guesses as to what's coming up in the future.

Since security issues are so critical, solutions are necessary on a here-and-now basis. In some cases, one minor security breach can bring down a major entity. So it would stand to reason that the persons most qualified to address security queries are the experts in the field who are dealing with up-to-the-minute threats. To address that premise, we posed four pressing security concerns to a roundtable of five top security professionals on the scene:

MD: Although sensors have been a critical component of most electronic devices, it has become obvious they will be deployed en masse via Internet of Things (IoT) applications. Equally obvious is the more applications you have online, the more opportunities for security and privacy breaches become available. Sensors in themselves are not vulnerable to security threats; however, the systems they interface with, i.e., data-acquisition boards, embedded systems, etc., are at risk. What IoT-type systems do you see as being the most vulnerable and why?

Vaughan Emery, CEO & President of CENTRI Technology believes, "the vast majority of IoT security practices today follow the same general design and technologies, making all systems vulnerable to the same attack types. However, critical infrastructure and financial services would likely be the most targeted by bad actors, making them the most vulnerable."

Alan Grau, President and Co-Founder of Icon Labs counters, "First, I would argue that sensors could indeed be a target for cyber-attack. Hackers have breached light bulbs and extracted network login credential from connected lightbulbs. Hackers could exploit the wireless interface on a sensor to send it bogus commands or steal data. I don't believe there is a single type of device that is most vulnerable. The devices that I am most concerned about are those that are not currently being scrutinized for security vulnerabilities. There are many vulnerable industrial and facility devices already in place that are now connected, without the required security in place to protect them. In addition, anytime someone develops and builds a device without carefully considering the attack vectors and ensuring counter measures are in place, they are almost guaranteed to develop a device that is vulnerable to attack."

Mille Gandelsman, CTO and Co-Founder of Indegy observes from a manufacturing perspective with, "Industrial control devices are the most widespread category of IoT devices, and were designed decades ago with no cyber security in mind. This is concerning since they are used to operate many different industrial and production processes in manufacturing plants and critical infrastructures. Therefore, they can impact people's lives. Imagine someone causing a power outage or altering the formulation of a drug. Industrial control networks lack visibility, their communication protocols are not encrypted and there are no authentication mechanisms embedded in them. These conditions make ICS IoT devices extremely vulnerable to threats."

Larry Stefonic, Founder at wolfSSL, sums things up compactly, "Sensor systems where an attacker has clear motivation are the most likely to have issues. Attackers get extremely clever when they are motivated!"

Scott Keller, President, SignalFire Telemetry Inc. points to the cloud. "The farther toward the cloud you are, the more the data is vulnerable as the concentration of data is higher and the interfaces are more easily hacked as they are more "standard". Field hacking is very difficult due to the (often) wireless nature of the interface and the protocols, themselves, are often proprietary and difficult to figure out. Many are also encrypted."

MD: There are some individuals in the industry and many end users who believe EOEMs are not doing enough to secure their products. In some cases, they feel manufacturers are putting products on the market, hoping no problems arise, but figure they will patch them as they surface. Two reasons for this approach are thought to be the pressure to get products to market [timetables are very narrow] and the cost of adding security to devices that may not have a long enough functional life. Do you agree with these thoughts? If so, what needs to be done by OEMs? If not, do you foresee other issues in this area?

More encompassing, Jon Stark, CEO of Peratech Holdco Limited, believes, "When products go through epidemic failure, they rarely come back. Let's use the hoverboard as an example. In 6 months, hoverboard sales went from the 10's of thousands to the millions and were on the verge of becoming an overnight household item last winter holiday season, when reports of battery failures began cropping up. And as fast as the market grew, it evaporated."

INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

SECURITY ROUNDTABLE:

What The Pros Know

He continues, **"Specifically, sensing solutions providers need to understand the potential security issues in hardware, firmware, and embedded software, all while addressing the realities of cost competitiveness.**

One way to ensure cost does not overshadow required security measures is for the IoT industry to push forward boldly on useful security standards for systems design, electronics, comms, protocols and embedded code."

Larry Stefonic answers, "At wolfSSL, we are fortunate in that we primarily deal with companies that care about their brands and their consumers. EOEM's come to us because they have made a conscious decision to secure their systems appropriately. As such, we have not seen a lot of the issues you describe."

On the other end, Vaughan Emery says, "I agree OEMs are not doing enough to secure IoT products. The most likely reason is that best practices and advanced security solutions are not well understood by the developers, product architects and product managers."

Taking a bit of center ground, Alan Grau injects, "I think these statements are generally but not universally true. Some OEMs are putting significant effort into ensuring their devices are secure. I do agree that this is **one of the most critical issues for IIoT Security. It has to be a priority and security has to be built into the device.** In some cases, I think market pressures will be enough to get OEMs to add security to their devices, but in other cases I think it will take regulation and standards to make OEMs focus on this issue. As long as security is not a priority, hackers will have an easy time penetrating these devices and networks."

Scott Keller believes that not all data is created equal. He states, "You have to look at what data you are transporting and how "important" it really is. If the data were to be corrupted, how much of an issue would that be? In some cases, it could be a big problem. These days, encryption algorithms are fairly easily obtained so adding it to a protocol is not too much of an issue. I would advise adding it for, if nothing else, marketing reasons."

Providing a solid solution, Mille Gandelsman states, **"Yes, I agree. Cyber security shouldn't be treated as something to be added later."** Security should be in the DNA of any company delivering ICS software or hardware products, and must be integrated at every step of the manufacturing process -- from research & design, through development and manufacturing. In addition, Cyber security defenses should also be implemented in ICS networks to protect IoT devices."

MD: There have been numerous debates over the vulnerability of open-source software that many companies freely use to drive their products. There are many bizarre imaginings of hackers taking over home appliances and trashing domiciles with explosions and fires. Is open-source code a security issue and to what extent? If not, what types of products are the safest bets for use with open-source software?

"Open source software isn't necessarily less secure," reveals Mille Gandelsman, "The fact that source code is freely available makes it easier for vulnerabilities to be discovered, but this also has a big positive effect – since flaws can be quickly published, addressed and patched. This is particularly true for software that is widely deployed, since the code is continually being inspected and fixed by a large population of users. Linux distributions are a good example. They are very safe."

"Again, you need to understand what the potential downside actually is," states Scott Keller. "I would be very worried about a hacker gaining access to my car but not the temperature of my refrigerator. Security needs to be put into perspective. I would not use open source for highly critical applicatons."

Jon Stark believes, **"We think having embedded software offers higher security,** as by nature there is no OS that offers extensibility. The drawback with embedded systems is that they are not nearly so intuitive to program. We have bridged this gap at Peratech with our Enrich IDE, a platform that generates standards-based, IC-agnostic code for embedded microcontrollers to be encrypted, compiled, and flashed at secure locations. With the right final functional test ensuring security measures, and even security in the boot sequence, sensor modules can be effectively secured. In addition, by being able to minimize the amount of code needed on the embedded controller, we fulfill the desire to select the most cost efficient MCU, as a by-product, we also provide security in not having extraneous resources to hack."

Verifying the necessity for open-source platforms, **"It is well recognized in the security community that open source is really the only way to do it,"** says Larry Stefonic. "Anyone who promotes obfuscation is doing so because they have a private agenda or something to hide. For those making security critical decisions, security software that is not open source should be a non-starter. To do security right, it takes a lot of input from a community that cares. For example, at wolfSSL, we get input on our code from every major vendor in computing, and every major research institution in cryptography. We couldn't get that kind of input if we were not open source."

Alan Grau concurs, "Any widely used software with known vulnerabilities is a security risk. There have been, and still are, known vulnerabilities in Microsoft Windows, Linux, OpenSSL and many other software packages. Regardless of the software solutions being used, it is important to ensure that vulnerabilities, once found, are patched. There must be a mechanism to ensure that devices in the field are rapidly updated when a vulnerability is found. There are thousands of devices in the field right now with known vulnerabilities that have not been upgraded. Some are devices using open source software and other are using commercial software. So while there is a risk in using open source software, that is only one of the factors that needs to be addressed."

INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

SECURITY ROUNDTABLE:

What The Pros Know

Vaughan Emery rounds it up with, "Open-source software is an essential part of nearly all software development projects; IoT product development is no exception. **However, the security-layer is NOT the best use of open-source because it provides bad actors with the know-how."**

MD: What do you see as the number one security concern facing manufacturers in the "happening-now" IoT?

Scott Keller points out, "I think that deploying a non-secure system in a secure application is the biggest problem. This is more a shortcoming of the integrator and not the product provider as the non-secure system may be designed for a non-critical application and the integrator may use it not understanding its security shortcomings."
Mr. Emery puts it bluntly, "The primary security concern for IoT manufacturers is how to prevent bad actors from killing their product in the market place."

Industrially speaking, Mr. Gandelsman concludes, "The biggest IoT security concern in my mind spans industrial processes and critical infrastructures across the globe, and is often referred to as IIoT or the industrial internet of things. Since IoT devices in SCADA and ICS infrastructures supervise critical processes including the manufacturing of pharmaceuticals, power generation, transmission and distribution, and even nuclear reactors… the consequences of a cyber-attack on these devices are extremely serious."

Briefly put, Mr. Stark states, "Attacks from the cloud or through poorly-secured wireless networks are my biggest concern."

Mr. Stefonic sees the number one security concern in threes,

(1) MITM, or Man in the Middle attacks
(2) Encrypting data on the device
(3) Secure firmware update

And Mr. Grau gets the last words, "Based on my discussions, the two biggest challenges are determining how much to invest in cybersecurity and what the best approaches are to securing their devices. These companies have many challenges and cybersecurity is seen as having a very low ROI, or no ROI at all. While they understand it is important they have trouble justifying the time and cost, especially given other priorities and market pressures. Once they decide to invest, there are many choices of what to invest in. What features and capabilities do they focus on? Building a comprehensive cyber-security approach is complex and costly, so many companies do a little and hope it is good enough. This is not a good approach."

An eBook from
Mat Dirjish, Executive Editor

sensors ONLINE
Your Technical Resource for
Sensing Communications & Control

INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

What to Do and What to Expect

After reviewing the studies and hearing what the experts have to say, it's clear that security issues are here, the threats are sophisticated, and growing on a daily basis. It should be equally clear that security, like good health, is something to be on top of religiously.

In the December 1, 2016 Issue of FORTUNE MAGAZINE, entrepreneur and noted SHARK Robert Herjavec offers three tips on

HOW TO IMPROVE YOUR COMPANY'S CYBERSECURITY

I. KNOW THE STATE OF YOUR NETWORK

Most breaches occur over time. Hackers want to get in and poke around for a while to learn the flow of your network. By the time you find out, they've already extracted data.

II. LOGS, LOGS, LOGS

Every time you hit a keystroke, it creates an electronic fingerprint. With the Internet of Things, the amount of data generated is incredible. We monitor far more than 100-billion logs daily. So make sure you have a way to correlate your logs in one place.

III. DO AN EXTERNAL AUDIT EVERY YEAR

Have a process to analyze your data, apply analytics, and have humans involved in it. Don't just rely on an internal team. Hire an outside firm for objective findings.

Founder of the Herjavec Group, Robert Herjavec points out three important ways to improve your cyberscecurity. The Herjavec Group is recognized as a global leader in information security specializing in managed security services, compliance, incident response, and remediation efforts for enterprise level organizations.

Predictions, Musings, and Ramifications

Although we could all live happily ever after without them, security threats do offer a wealth of opportunities for defenders of the enterprise. There is certainly no shortage of security providers to choose from. These providers offer everything from basic network and email protection to complex encryption and data-coding algorithms. Just see the short list of 500 US companies linked from the figure below.

When it comes to security issues on a daily basis, it's never a matter of if an attack, hack, or hijack will occur, it's a matter of when and what. Addressing the timing of a security breach could be tricky, however it should seem obvious that the answer is anytime 24/7. Therefore, round-the-clock protection and vigilance is in order.

What form the attack takes is probably the hardest to foresee as the hackers' skills are in a constant state of evolution to meet the challenges of the equally morphing skills of the security people. Sometimes though, the hackers seem to be getting faster, sneakier, and more clever. Clearly it's in the enterprise's best interest to keep abreast of what's happening in related and unrelated industries.

There are market studies done on a regular basis as to what types of security issues are arising, reports of industry breaches large and small, and a plethora of resources available for free. This report you are reading has links to several such studies and Sensors Magazine covers up to date studies and surveys in its daily and monthly embedded news coverage and newsletters. Again, there will be a wealth of security coverage at both Sensors Expo & Conference 2017, West and Sensors Midwest 2017.

Getting predictions from security professionals are always worth more than just a passing glance. McAfee labs is one such source. The company is a household name when it comes to personal-computer security products for the consumer, pro, and enterprise playing fields. They offer a range of software products and, partnering with Intel Security, free threat reports on their website.

As far as what the near future has in store, Intel Security's McAfee Labs 2017 Threats Predictions Report pinpoints 14 threats to keep an eye on. These threats are the culmination of opinions on current trends in cybercrime from 31 Intel security professionals. See figure 9 for the company's 14 security developments for 2017 predictions.

The report also zeroes in on several other key security issues. These include cloud security, IoT predictions, and critical industry challenges. The full report from Intel Security is available for download in PDF format.

McAfee®
An Intel Company

McAfee Labs predicts 14 security developments for 2017

1. Ransomware attacks will decrease in volume and effectiveness in the second half of 2017.
2. Windows vulnerability exploits will continue to decline, while those targeting infrastructure software and virtualization software will increase.
3. Hardware and firmware will be increasingly targeted by sophisticated attackers.
4. Hackers using software running on laptops will attempt "dronejackings" for a variety of criminal or hacktivist purposes.
5. Mobile attacks will combine mobile device locks with credential theft, allowing cyber thieves to access such things as banks accounts and credit cards.
6. IoT malware will open backdoors into the connected home that could go undetected for years.
7. Machine learning will accelerate the proliferation of and increase the sophistication of social engineering attacks.
8. Fake ads and purchased "likes" will continue to proliferate and erode trust.
9. Ad wars will escalate and new techniques used by advertisers to deliver ads will be copied by attackers to boost malware delivery capabilities.
10. Hacktivists will play an important role in exposing privacy issues.
11. Leveraging increased cooperation between law enforcement and industry, law enforcement takedown operations will put a dent in cybercrime.
12. Threat intelligence sharing will make great developmental strides in 2017.
13. Cyber espionage will become as common in the private sector and criminal underworld as it is among nation-states.
14. Physical and cybersecurity industry players will collaborate to harden products against digital threats.

An eBook from
Mat Dirjish, Executive Editor

sensors ONLINE
Your Technical Resource for Sensing Communications & Control

INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

The Penultimate Word

In parting, there is one other study to consider, one offered by the Information Systems Security Association (ISSA) and independent industry analyst firm Enterprise Strategy Group (ESG). Claiming the Cybersecurity Profession is at Risk, the study in question found two concerns. First, most cybersecurity professionals aren't receiving the right level of skills development to address the rapidly evolving threat landscape. Second, the skills shortage has created a job market that represents an existential threat, adding job-related stress to cybersecurity personnel while making it harder for organizations to protect critical IT assets.

So all this leads us to a few observations and revelations. Simply put, cyber-security professionals are very much like folk singers. In the case of folk singers, if war, poverty, unemployment, prejudices, and injustices did not exist, they would be out of a job. If there were no hackers, phishers, spammers, fake international lotteries, and money-transfer schemes, the cyber-security pros would be out of work. Even worse, they might become folk singers. Using part of Mr. Vaughan Emery's favorite expression, we do not need anymore "bad actors". **~MD**

INTRO & TOP FINDINGS

SECURITY EVOLUTION

SECURITY PRESENT

WHAT THE WARNING STUDIES SAY NOW

ON THE OTHER HAND

SECURITY ROUNDTABLE

WHAT TO DO AND WHAT TO EXPECT

PREDICTIONS, MUSINGS, AND RAMIFICATIONS

THE PENULTIMATE WORD

COMPANY PROFILES

CONTACT

REFERENCES

Company Profiles

CENTRI Technology ~ CENTRI provides advanced security for the Internet of Things. The company's technology helps organizations secure their data by seamlessly integrating into existing applications and services in the cloud, data centers, connected devices, and products. By establishing trusted devices and advanced encryption while retaining complete visibility to data, CENTRI eliminates the risk of data exfiltration and loss of equipment command.

www.centritechnology.com

Icon Labs ~ Icon Labs provides cross platform security solutions for embedded OEMs and IoT device manufacturers. Solutions support all major embedded operating and real-time operating systems with security modules designed specifically for use in limited resource environments common to the embedded marketspace. These solutions provide security building blocks for protecting the device itself rather than just relying on security at the perimeter.

www.iconlabs.com

Indegy ~ The Indegy team combines cyber-security expertise with hands-on industrial-control knowledge. The company's platform enables users to secure and control ICS networks by mapping all the controllers on the network, documenting their configuration, logging all activities and changes, and providing visibility into to their state.

www.indegy.com

Peratech Holdco Limited ~ Peratech is a force-sensing HMI/MMI company and inventor/developer of proprietary Quantum Tunnelling Composites (QTC) materials. Providing next-generation touch-/force-sensing solutions, the company's core IP is protected by a divers international patent portfolio.

www.peratech.com

wolfSSL ~ wolfSSL provides lightweight, portable security solutions with a focus on speed and size. The company is dual-licensed to cater to a diversity of users. Its products are open source, giving users the freedom to inspect the codebase first hand.

www.wolfssl.com

SignalFire Telemetry Inc. ~ SignalFire's patent-pending two-way mesh technology enables reliable data transfer over long node-to-node distances. Its unique message-forwarding architecture creates an affordable system that's easy to deploy. The technology is viable for applications requiring many assets widely dispersed at distances up to four miles point-to-point, such as flow, level, pressure, and temperature devices.

www.signal-fire.com

An eBook from
Mat Dirjish, Executive Editor

sensors ONLINE
Your Technical Resource for
Sensing Communications & Control

INTRO & TOP FINDINGS
SECURITY EVOLUTION
SECURITY PRESENT
WHAT THE WARNING STUDIES SAY NOW
ON THE OTHER HAND
SECURITY ROUNDTABLE
WHAT TO DO AND WHAT TO EXPECT
PREDICTIONS, MUSINGS, AND RAMIFICATIONS
THE PENULTIMATE WORD
COMPANY PROFILES
CONTACT
REFERENCES

For our 2017 Digital E-Book Series, is there research you'd like to see?

Contact:

Mat Dirijsh
Executive Editor
(718) 793-5501 • mdirijsh@questex.com

www.sensorsmag.com

Learn more by attending Sensors Events:

- In-depth technical sessions
- Dedicated education on IoT, Embedded Systems & Sensors, and Security
- Best-in-class exhibitors showcasing the latest technologies
- Key technology Pavilions, including IoT and Embedded Systems
- Hands-on workshops
- And more!

sensors expo & conference

June 27-29, 2017
McEnery Convention Center
San Jose, California
www.sensorsexpo.com

sensors MIDWEST

October 2-4, 2017
Donald E. Stephens Convention Center
Rosemont, Illinois
www.sensorsmidwest.com

Mat Dirjish is the Executive Editor of Sensors Magazine. Before coming on board, he covered the test and measurement and embedded systems market, as well as the electronic components market, for a variety of industry publications. He also has an extensive background in high-end audio/video design, modification, servicing, and installation.

REFERENCES

Related Security Surveys, Findings, And Stories:

U.S. Grid in 'Imminent Danger' from Cyberattack
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/us-grid-imminent-danger-cyberattack-24590]

Mass Surveillance Is Cybersecurity's No. 1 Threat
[http://www.sensorsmag.com/sensors-products/embedded-systems/news/mass-surveillance-cybersecuritys-no-1-threat-24557]

CEOs Reveal Cyber Naivete
[http://www.sensorsmag.com/sensors-products/embedded-systems/news/ceos-reveal-cyber-naivete-24558]

Cloakware Receives Frost & Sullivan Award for New Product Innovation
[http://www.sensorsmag.com/automotive/comfort-safety/news/cloakware-receives-frost-sullivan-award-new-product-24542]

Japanese Company Replaces Office Workers with Artificial Intelligence
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/japanese-company-replaces-office-workers-artificial-24545]

Argus Announces Automotive Cyber Security Solution Powered by Qualcomm Technologies
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/argus-announces-automotive-cyber-security-solution-powered-24506]

Manufacturers Behind in Preparing for Cyberthreats
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/manufacturers-behind-preparing-cyberthreats-24483]

Federal Information Security Spending to Reach $12B by 2021
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/federal-information-security-spending-reach-12b-2021-24438]

Security Concerns over Re-use of Personal Credentials
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/security-concerns-over-re-use-personal-credentials-24439]

Safety and Comfort Drive Smart Home Purchases
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/safety-and-comfort-drive-smart-home-purchases-24421]

Consumers Fear Cyberattacks Disrupting Celebrations
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/consumers-fear-cyberattacks-disrupting-celebrations-24422]

RUAG Acquires Cyber Security Specialist Clearswift
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/ruag-acquires-cyber-security-specialist-clearswift-24407]

Analyst Firms Name IBM a Leader in Software Testing Capabilities
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/analyst-firms-name-ibm-leader-software-testing-capabilities-24409]

Report Reveals Impact of Cybersecurity Skills Shortage
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/report-reveals-impact-cybersecurity-skills-shortage-24392]

Contrast Security Makes .NET Applications Self-Defending
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/contrast-security-makes-net-applications-self-defending-24393]

Cyberbit Increases Security Operations Efficiency With New SOC 3D Release
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/cyberbit-increases-security-operations-efficiency-new-soc-3d-24394]

Businesses More Likely to Pay Ransomware than Consumers
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/businesses-more-likely-pay-ransomware-consumers-24375]

IEEE and Barr Group Emphasize the Importance of Software Safety
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/ieee-and-barr-group-emphasize-importance-software-safety-24376]

'Human' Issues Is Top Cybersecurity and Business Risk
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/human-issues-top-cybersecurity-and-business-risk-24363]

Proficio Partners with CrowdStrike to Provide Advanced Managed Endpoint Security Services
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/proficio-partners-crowdstrike-provide-advanced-managed-24367]

Security Vendors Under Pressure to Offer Cyber Guarantees
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/security-vendors-under-pressure-offer-cyber-guarantees-24345]

Increasing Security Threats to Fuel Airport Passenger Screening Systems Market
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/increasing-security-threats-fuel-airport-passenger-screening-24346]

Nearly Half of All Websites Pose Security Risks
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/nearly-half-all-websites-pose-security-risks-24316]

CounterTack Joins IBM Security App Exchange Community
[http://www.sensorsmag.com/sensors-products/embedded-systems/news/countertack-joins-ibm-security-app-exchange-community-24317]

McAfee Labs Report Finds 93 Percent of Security Operations Center Managers Overwhelmed by Alerts and Unable to Triage Potential Threats
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/mcafee-labs-report-finds-93-percent-security-operations-24298]

Vertiv Identifies Data Center Infrastructure Trends for 2017
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/vertiv-identifies-data-center-infrastructure-trends-2017-24299]

Study Highlights Need for Actionable Cyber Awareness
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/study-highlights-need-actionable-cyber-awareness-24238]

Americans Taking EMV Shift in Stride
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/americans-taking-emv-shift-stride-24240]

IoT Tops 2017 Global Security Threat Outlook
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/iot-tops-2017-global-security-threat-outlook-24245]

NYU Cybersecurity Students Devise a New Way to Safeguard Electronic Voting Systems
[http://www.sensorsmag.com/news/tech-product/news/nyu-cybersecurity-students-devise-new-way-safeguard-24281]

Study Finds Clear Patterns in Bad Passwords
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/study-finds-clear-patterns-bad-passwords-24282]

How Americans Feel About Cybersecurity
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/how-americans-feel-about-cybersecurity-24283]

Can Blockchain Technology Secure Digital Voting Systems?
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/can-blockchain-technology-secure-digital-voting-systems-24285]

Study Highlights Need for Actionable Cyber Awareness
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/study-highlights-need-actionable-cyber-awareness-24238]

Americans Taking EMV Shift in Stride
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/americans-taking-emv-shift-stride-24240]

IoT Tops 2017 Global Security Threat Outlook
[http://www.sensorsmag.com/electronics-computers/embedded-systems/news/iot-tops-2017-global-security-threat-outlook-24245]

An eBook from
Mat Dirjish, Executive Editor

sensors ONLINE
Your Technical Resource for Sensing Communications & Control

INTRO & TOP FINDINGS

SECURITY EVOLUTION

SECURITY PRESENT

WHAT THE WARNING STUDIES SAY NOW

ON THE OTHER HAND

SECURITY ROUNDTABLE

WHAT TO DO AND WHAT TO EXPECT

PREDICTIONS, MUSINGS, AND RAMIFICATIONS

THE PENULTIMATE WORD

COMPANY PROFILES

CONTACT

REFERENCES