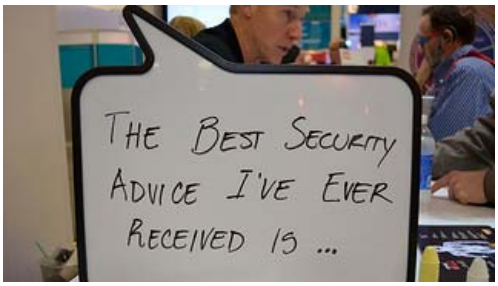
20 of the Best IT Security Lessons Ever Learned

DAVID SPARK (HTTPS://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/DAVID-SPARK/)

MAY 1, 2012 | IT SECURITY AND DATA PROTECTION (/STATE-OF-SECURITY/TOPICS/SECURITY-DATA-PROTECTION/)



(http://www.flickr.com/photos/tripwireinc/6950168297/in/set-72157629140337926/)After working in information security for many years, we've come to understand that *change* is infosec's only constant. Systems, people, and the secure state of your company, the network, and its data are always in flux.

To keep up with the IT security's ever-changing nature, we reached out to experts and practitioners to see if they could pass on what they've learned. We simply asked, "What's the best advice you ever learned about IT security?"

What follows is a list of the best advice from security gurus, network administrators, and those responsible for securing company information. The lessons were passed down to them from real-world experience, a supervisor, an industry colleague, or in one case, a complete stranger.

Tip #1: Security must *enable* business, not prevent it

"I don't know anything about what you do, for all I know, you are doing your job perfectly, but you have disabled my ability to do my job," said a company executive to Stewart Allen (http://www.stewartallen.com/), now an Information Security Consultant at Metrolinx (http://www.metrolinx.com/).

Not immediately understanding the impact of that statement, Allen shot back with the retort, "Yes I am doing a good job. Our data is secure. So deal with it."

The executive responded, "Well Stewart, I issue you a challenge! Find a way to use your security skills to enable business people like myself to work

better, while still keeping our information secure."

Allen admitted he initially ignored the comment, but it played in his mind for weeks until he came in one weekend and rewrote the entire firewall policy to enable business flexibility while still keeping data secure.

The executive's challenge changed his career. He wouldn't be the consultant he is today if it weren't for that advice. As a result, Allen's security motto is: "I enable business through the effective use of information security practices."

Here's a video we shot at the 2012 RSA Conference where we asked attendees, "What's the best security advice you've ever received?"

Tip #2: Work with people. Don't fight them.

"Technology has come to a point (almost) where the employees don't need the IT department. So the security professionals are fighting to keep the employees in and it is like trying to hold a handful of water. They do what they want to," realized Kevin Jones (@KevinDJones (http://twitter.com/KevinDJones)), Social Media Strategist for NASA (http://www.nasa.gov/)/Dynetics (http://www.dynetics.com/).

“We try so often to fight against people and put in place more technologically advanced systems,” said Jones. “If you want to keep your information secure, work with the people.”

“Working with the people” means understanding users’ motivation and behavior. “What’s the reasoning behind why they do what they do,” said Jones.

It’s not easy to come to agreement, admitted Jones, who has taken months to work with security in *partnership* to take down the walls, understand the user more intimately, and thus change the traditional security perspective.

Echoing the need to understand users’ motivations, Daniel Blander (@djbphaedrus (http://twitter.com/djbphaedrus)), President of Techtonica, Inc. (http://www.techtonica.com/), has been moved by the advice of motivational speaker, Tony Robbins (http://www.tonyrobbins.com/) about understanding people’s basic motivations, such as issues of certainty, uncertainty, significance, love, connection, growth, and contribution.

“I use [Robbins’ advice] every day in my consulting and my day-to-day activities so I can understand someone’s motivations, and temper my frustration with bad behavior,” said Blander.

Tip #3: Problems first, then solutions

(http://www.flickr.com/photos/tripwireinc/6950173641)“Don’t try to find a solution until you’ve understood the problem,” advised a veteran IT executive to Norman D. Marks (@normanmarks (http://twitter.com/normanmarks)), VP, Evangelist for Better Run Business at SAP (http://sap.com/).

“From an IT security perspective, this

means that you need to understand the risk before determining the level of security measures to apply," said Marks.

When Marks was at Solectron, the lead managers for both physical and IT security wanted Marks to solicit funds to encrypt all the executive laptops across the company. While that sounded like a worthwhile endeavor, Marks asked if they had completed a corporate-wide information security risk assessment. They hadn't. Instead of just accepting the seemingly reasonable request, Marks researched the situation only to discover that basic user access provisioning was broken.

"They wanted to close the windows when the front and back doors were open," realized Marks.

Tip #4: Teach the basics again and again

(http://www.flickr.com/photos/tripwireinc/6804063318/in/set-72157629140337926/)"Never be afraid to discuss the simplest things—things you may think are already known, or that you consider common sense—and repeat them frequently," said Aryeh Goretsky (@goretsky (http://twitter.com/goretsky)), Distinguished Researcher at ESET (http://eset.com/).

Instead of chasing the latest and greatest threat, a common practice in the security field, you can be far more effective just educating personnel about simple secure practices, over and over again, said Goretsky.

"It can be easy to forget about doing the most basic security things right," echoed Jacob Kitchel (@i_defender (http://twitter.com/i_defender)), Senior Manager of Security and Compliance at Industrial Defender

(http://www.industrialdefender.com/). "Taking care of the basics first, and ensuring sufficient logging, has allowed me to help customers 'right the ship' and gain perspective on what exactly is happening in their environments."

Tip #5: Data security and privacy starts with employees

(http://www.flickr.com/photos/tripwireinc/6950173015/in/set-72157629140337926/)"It doesn't matter what firewall or intrusion detection you use if your employees don't understand the significance of data privacy and protection," said Anthony R. Howard, IT consultant and author of "The Invisible Enemy: Black Fox." (http://anthonyrhoward.com/)

"No one in your organization will care about data security, privacy policies, intellectual property protection, or data breach until you tell them why it's important, how it can impact *them*, and then tell them what to do to prevent it," advised Howard who suggests basic training, such as a webinar, to explain how they personally can protect themselves and their company from data theft.

What you ultimately want to do is create a mutually beneficial privacy culture that can be applied to both your business, and the employees' personal life, said Howard.

Tip #6: Mistakes happen, especially by you

(http://www.flickr.com/photos/tripwireinc/6804062316/in/set-72157629140337926/)"Trust no one, especially yourself. Check, recheck, check again," was the advice a physical security professional gave to Catalin Tutunaru (http://no.linkedin.com/in/catalintutunaru),

a freelance ICT consultant.

The advice has been a backbone of Tutunaru's consulting business as he realizes there's an inherent unavoidable weaknesses in the people hired to protect networks.

"The ICT community is very young and the experience collected is much smaller than the power they control," Tutunaru said.

Tip #7: To get respect, you'll need a few shots fired at you

"You won't be truly appreciated until you manage a security breach," said Sean Jackson (@shunkydave (http://twitter.com/shunkydave)), Security Engineer at DigiCert (http://digicert.com/) who learned that advice from a fellow security professional.

"I immediately changed my focus from preventing the unknown to preparing to manage what I did know," said Jackson.

Tip #8: Think like an attacker

"Good security isn't a set of tools," said Andrew Jaquith (@arj (http://twitter.com/arj)), CTO of Perimeter E-Security (http://perimeterusa.com/), "It's a mindset."

While working at @stake (http://en.wikipedia.org/wiki/@stake), a security consultancy Jaquith helped found in 1999, he learned from his colleagues and watching guys at the hacker collective, L0pht (http://www.l0pht.com/), to always put yourself in the attacker's shoes when thinking about security.

"It's not about checking the box, making the auditor happy or following 'best practices.' It's about repelling the wily hacker," said Jaquith who used this 'put

yourself in the attacker's shoes' attitude to work, by trying to break into systems.

"There was not a system our people couldn't get into, and it all came back to that single point: having the right mindset," said Jaquith. "We used the insights we gained from successful attacks to help our customers be more secure."

Tip #9: Backup your data…away from the data source

(http://www.flickr.com/photos/tripwireinc/6950169045/in/set-72157629140337926/)Early in his security career as a Linux sysadmin, Anton Chuvakin, (@anton_chuvakin (http://twitter.com/anton_chuvakin)), Research Director at Gartner (http://gartner.com/) learned, "Everything will fail: prevention, detection, response, the data center will explode, the DoS will flood your connection, auditors will find fault, and attackers will steal your fighter plans. But you will always have *backups*! Which means you can always get back to life."

Not all backups are equal though. For months, Jay Walker (@Conteggo (http://twitter.com/conteggo)) was backing up his laptop on a thumb drive and kept both the laptop and the USB drive in his laptop bag. He was so proud of himself for being so conscientious until a stranger advised him as to how foolish a practice that was. If he ever lost that bag, he'd be fried.

Soon after that conversation, that scenario, through theft, happened to a family member. That stranger's advice indirectly led to him launching his online backup service company, Conteggo (http://conteggo.com/).

Tip #10: If it's online, you can't be certain it's private

(http://www.flickr.com/photos/tripwireinc/6804062874/in/set-72157629140337926/)"Never assume anything you put on the Internet is private, even if it hasn't been shared with anyone," said Josh Ogle (@joshogle (http://twitter.com/joshogle)), Founder of Fresh Spin Advertising (http://freshspinads.com/) who believes this personal tenet has had a demonstrable impact on his business and career.

Working in advertising, Ogle has clients who entrust their very sensitive intellectual property to his company. When they pitch a client they make it clear they will never put anything sensitive of theirs online, and he knows of two occasions where that differentiator led companies to choose his boutique ad agency over competitors.

Tip #11: In a business vs. security battle, business is always right

(http://www.flickr.com/photos/tripwireinc/6950168689/in/set-72157629140337926/)"When security gets in the way of the mission, security is wrong, not the mission," said Keith Palmgren (@kpalmgren (http://twitter.com/kpalmgren)), President of NetIP (http://www.netip.com/).

"In the corporate environment, the fundamental mission is revenue," said Palmgren. "Put security in place that

prevents revenue generation and the boss will tell you exactly how wrong you are and how little time you have to fix it."

Watching others make this misstep many times, Palmgren quickly learned that repeatedly hindering the business with security can be a career limiting move.

Tip #12: A business must balance some risk in order to profit

When Patrick C Miller (@PatrickCMiller (http://twitter.com/patrickcmiller)), President and CEO of the Energy Sector Security Consortium (http://energysec.org/), was a young and overzealous security pro, an executive at another company once said to him that his answer to every project, initiative, and "Can we do this?" question was always "no." Eager not to be hindered by security, the executive challenged Miller.

"What I want to hear is: 'yes, if' instead of 'no,'" said the executive.

Miller finally realized that the organization is balancing risk in order to profit and it changed his complete outlook of how he communicates.

"I was finally able to speak to the executive layer in a language they would understand and respond to – which never happened when I spoke in technical security terms," Miller said.

(http://www.flickr.com/photos/tripwireinc/6950173265/in/set-72157629140337926/)"You have to accept that fact that as a security professional you can't always get what you want, but you can help the business get what it needs," said Andrew Storms (@st0rmz (http://twitter.com/st0rmz)), Director of Security Operations for nCircle (http://ncircle.com/), who had a similar enlightened experience as Miller.

"Your job as a security professional is to

in help the business understand the role information security risk plays in the way your specific organization conducts its business," said Storms who now thinks more strategically about how he frames conversations about security with executives.

TIP #13: Business first, then security

Similar to the previous tip is the importance of first knowing what you've been hired to protect.

"It's important to understand the business before you can secure it," said Terry L. Perkins, who does information security at a large resell bookstore.

To build appropriate, justifiable defenses around information assets, Frank Marsh, Director of Cyber and Information Security at Burrill Green (http://www.burrillgreen.com/), advises, "Understand *what* information drives your business or organization, *where* it is (both digitally and physically), and *why* it needs protecting."

TIP #14: Educate users about good password security

(http://www.flickr.com/photos/tripwireinc/6950170823/in/set-72157629140337926/)Heeding advice from notorious hacker, Kevin Mitnick, Bill Bernat (@microvation (http://twitter.com/microvation)), Web Publisher at OpenText (http://opentext.com/), focuses on basic password security. For starters that means use unique/random passwords – no "God" passwords for multiple accounts, no writing passwords on PostIt notes, no sharing passwords, and no saying them out loud on the phone or over email.

For Bernat, the advice has meant he's never made any *huge* mistakes.

"You could build the most brilliant system ever and if you don't make backups or change the default password that could kill your career in an afternoon," warned Bernat.

Tip #15: Be wary of how much authority you give to a consultant

Even if you're a small company that doesn't fully understand how your IT project functions, don't give all the power to a programming consultant, advised Diana Moy (@arteefact (http://twitter.com/#%21/arteefact)), Visual/Information Designer at Artefacts.us (http://artefacts.us/) who has seen her clients' operations be completely vulnerable to the unpredictability of a consultant.

You never know what could happen, said Moy. A programmer could get sick, disappear, or simply walk away with your code and content. Protect your business by setting up your system so that you have master control over the web server and database.

"If you're an IT professional, make sure you give this advice to your client. It's a good way to build trust," said Moy.

Tip #16: Don't go overboard

(http://www.flickr.com/photos/tripwireinc/6804057002/in/set-72157629140337926/)"While I do not underestimate the need for solid IT security measures, I also know that you can overdo it," said Gyutae Park (@MoneyCrashers (http://twitter.com/MoneyCrashers)) Head of IT for Money Crashers Personal Finance (http://www.moneycrashers.com/).

Even after covering all the basics of securing his network, Park still gets solicitations from software sales reps

telling him about the importance of a certain product or why he needs to install a certain piece of software.

“Too much security software can bog down your operating system, and it can be quite costly. I need to save money for my business (http://www.moneycrashers.com/cost-cutting-ideas-small-business-expenses/) in any way possible,” said Park. “Playing it simple but safe in regards to IT security is one way to do that.”

Tip #17: Make the cost of breaking in higher than the benefit

(http://www.flickr.com/photos/tripwireinc/6950169273/in/set-72157629140337926/)One hundred percent security is an impossibility as most security pros have come to accept. “If someone wants to break in bad enough, eventually they will,” said Dave Sroelov,President at A & S Computer Services (http://www.ascomputer.com/wordpress/).

“Make the effort of breaking into your systems and data much higher than any potential rewards gained by it,” said Matthew Hemmings (@RockfordIT (http://twitter.com/rockfordIT)), 3rd Line Technical Support/Systems Team at Rockford IT (http://www.rockford-it.co.uk/).

“There are only two things you can do about [managing your data security],” said Sroelov of dealing with intruders to your network. “First, make it as difficult as possible, and second, make sure they leave a trail behind them.”

Tip #18: Record as much activity as you can

Echoing Sroelov’s last piece of advice in the previous tip, Kitchel of Industrial

Defender advises companies to “squeeze every bit of information out of your environment. Log and record every event that you have disk space for. Then buy more disk space and log some more.”

“You may not be a security wizard or have one employed in your organization,” said Kitchel, “But when something goes wrong and you have to hire professionals to figure it out, extensive event logging will allow the pros to more easily figure out the pieces.”

Tip #19: Destroy and recycle electronics correctly

We focus so much data security effort on the equipment that’s currently being used to access our network. But what about the devices that are no longer sharing data, but have data on them, such as old cell phones, photo copiers, computers?

“While this data may have been stored in a hardened, protected environment through its lifetime, [but once decommissioned] it would now be in the wild and open to anyone with the know-how to recover improperly-wiped data,” said Brian Brundage, CEO of Intercon Solutions (http://interconrecycling.com/).

“Dispose [your devices] through a process that tracks and verifies the destruction of your data, from pick-up to physical destruction,” said Brundage whose company offers this very recycling service.

Tip #20: Security is everyone’s responsibility

(http://www.flickr.com/photos/tripwireinc/6950166821/in/set-72157629140337926/)While all of this security advice is useful, it’s important to understand that security is not one person’s job for others to not

worry about. It's everyone's responsibility and therefore everyone is susceptible to the same weakness.

"We can have the best policy, the best processes, and the best procedures using technologically sound tools yet still be vulnerable to the biggest security problem of all – humans," said Adam Montville (@adammontville (http://twitter.com/adammontville)), Security and Compliance Architect for Tripwire (http://tripwire.com/).

Montville learned this valuable lesson while working at the Department of Defense after yet another "out-of-policy" incident occurred. Shaking his head with a "not again" realization, the DoD's Information System Security Manager let Montville know, "This happens far more often than you might imagine, and it's because humans are still humans wherever you go."

"All the electronic locks and passkeys won't help if you hold the door open and let someone through with you," said Heather Wilde (@heathriel (http://twitter.com/heathriel)) Director of Technical Support for Evernote (http://evernote.com/). "Personal responsibility is the most important tool in the security arsenal. Security starts and ends with *you*."

Conclusion: What's the best infosec lesson you've learned?

(http://www.flickr.com/photos/tripwireinc/6804064286/in/photostream/)We're sure we haven't covered every single piece of useful advice. Heck, here's one right now:

Install patches and updates.

Still, with all the advice we know that's missing, we wrote this article in an effort to share the knowledge, wisdom, and

experience of fellow IT security pros, and we hope it sparks a discussion here in the comments.

Please, if you've got a piece of advice that tags on to one of the above 20 tips or is one of your own, let us know. We'd all like to learn and better protect ourselves and our businesses. Thank you.

25

CATEGORIES IT SECURITY AND DATA PROTECTION (/STATE-OF-SECURITY/TOPICS/SECURITY-DATA-PROTECTION/)

TAGS

About David Spark

(https://www.tripwire.com/state-of-security/contributors/david-spark/)

David Spark (https://www.tripwire.com/state-of-security/contributors/david-spark/) has contributed 156 posts to The State of Security.

View all posts by David Spark ›

Enter your email address here...

Sign Up

FREE EBOOK

(http://www.tripwire.com/scm/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies)

Security Configuration Management For Dummies (http://www.tripwire.com/scm/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies)

Download Now (http://www.tripwire.com/scm/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-f

Latest Security News (/state-of-security/topics/latest-security-news/)

Canada to Enact Legislation that Will Require All Businesses to Report Data Breaches FEB 17, 2017

Rasputin Hacker Uses SQLi to Hack 60 Universities and Government Agencies FEB 16, 2017

Romance Scams Cost Victims $230M in 2016, Reports FBI FEB 15, 2017

New Proof-of-Concept Ransomware Can Target PLCs at Industrial

Sites FEB 14, 2017

Man Jailed Indefinitely for Refusing to Decrypt Hard Drives FEB 13, 2017

FEATURED RECENT

(https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/raking-ransoms-russian-ransomware-threat-landscape-ticks/)

Raking in the Ransoms: How the Russian Ransomware Threat Landscape Ticks (https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/raking-ransoms-russian-ransomware-threat-landscape-ticks/)
FEB 16, 2017

(https://www.tripwire.com/state-of-security/featured/more-yahoo-users-warned-of-malicious-account-access-via-forged-cookies/)

More Yahoo users warned of malicious account access via forged cookies (https://www.tripwire.com/state-of-security/featured/more-yahoo-users-warned-of-malicious-account-access-via-forged-cookies/)
FEB 16, 2017

(https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/cyber-insurance-coverage-concerns/)

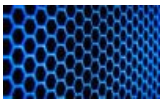
Cyber Insurance Coverage Concerns (https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/cyber-insurance-coverage-concerns/)
FEB 15, 2017

(https://www.tripwire.com/state-of-security/tripwire-news/new-research-highlights-

New Research Highlights Top Cyber-Attack Concerns for 2017 (https://www.tripwire.com/state-of-security/tripwire-news/new-

top-cyber-attack-concerns-for-2017/)

research-highlights-top-cyber-attack-concerns-for-2017/)
FEB 15, 2017



(https://www.tripwire.com/state-of-security/ics-security/4-tips-successful-ot-security-marriage/)

4 Tips for a Successful OT & IT Security Marriage (https://www.tripwire.com/state-of-security/ics-security/4-tips-successful-ot-security-marriage/)
FEB 14, 2017

(http://bit.ly/1Kb6rne)

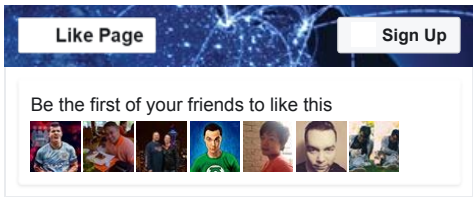
Tweets by @TripwireInc

Tripwire, Inc. @TripwireInc
Cyber Insurance Coverage Concerns tripwire.me/2kS5u1o via @SBLTD #security #cyber

Cyber Insurance Coverage Concerns
Cyber insurance can be part of a securit…
tripwire.com

1h

Embed View on Twitter



Topics (/state-of-security/topics/)

- Government
- ICS Security
- Incident Detection
- IT Security and Data Protection
- Latest Security News
- Off Topic
- Regulatory Compliance
- Risk-Based Security for Executives
- Security Awareness
- Security Slice
- Tripwire News
- Vulnerability Management