FOCUS

Focus IT Roundtable:
Security Gotchas that are Often Overlooked in SMBs

Focus Research, Inc

Moderator: Kevin Beaver
August 12, 2011
1pm PT

About the Roundtable:
Focus Expert Roundtables are 45 minute teleconferences where 3-5 members of the Focus Expert Network talk about hot topics on a particular category each week. On August 12, 2011 Focus Experts Andrew Baker, Kevin Beaver, Erik Goldoff and Fred Stuck sat down to address the security threats many small to mid-sized businesses overlook and offered advice on how to substantially mitigate these risks.

Kevin Beaver — All right, thanks and welcome, everybody. Welcome to the Focus Roundtable - Security Gotchas that are Often Overlooked in SMBs. Focus.com's 5,000 industry experts help millions of professionals make better business and technology decisions by answering questions, publishing research, and speaking at events.

Visit Focus.com to learn more and become a member today. And please visit our event page at www.focus.com/events to post and view comments and/or questions that you may have for this event.

So let's jump right in. My name is Kevin Beaver and I'm going to be your moderator today. My background is in IT. I've been an IT for about 22 years and I've been focusing on information security for the past 16 years. My company name is Principle Logic. I am based in Atlanta and businesses hire me to perform independent security assessments.

Basically, to point out the flaws in their network operations, their web applications, the general network environment. I've written a few books on the subject, including Hacking For Dummies. And I write a lot of other articles and I have a blog called The Security on Wheels Blog where I write about what I think are timely topics, including small and medium sized business security-related issues.

And you can follow me on Twitter at @kevinbeaver. So enough about me. The real brains are the other guys on the line. We've brought together some of the top focus experts in this area to share their insights on Security Gotchas that are Often Overlooked in SMBs. We have Andrew Baker, Erik Goldoff, and Fred Stuck.

And, guys, why don't you take a few moments and introduce yourselves to our listeners? Andrew, why don't you start out?

Andrew Baker — Thank you very much, Kevin. My name is Andrew Baker. I'm a hands-on information technology leader with expertise in designing, deploying, and maintaining secure networks for enterprises of all sizes. For over a decade, I have set technology strategy and led tech teams in mitigating risk, streamlining operational processes and solving critical business problems in a cost effective way.

I'm also an avid open net-worker. You can find my profile on Focus and you can also find me at zxeeme.com/andrewbaker. That's zxeeme.com/andrewbaker.

Kevin Beaver — Excellent. Thanks, Andrew. Eric?

Erik Goldoff — Good afternoon, I'm Erik Goldoff; also in the Atlanta area, so I'm surprised I haven't met you yet. I have been in IT field for some twenty-five years, very dynamic field, and principally working in small and medium business for about the last 10 years up until the last month or so.

So, I've got a lot of experience at the SMB level in addition to the very large enterprise federal. I do IT systems and security and especially focusing on making effective use of the budget in implementing security.

Kevin Beaver — Excellent. Thanks, Erik. And Fred.

Fred Stuck — Thanks. Hi, everyone. I'm Fred Stuck. I'm a network security engineer. I have over 10 years of experience. I've worked on a variety of both large and smaller organizations. I have experience primarily with Cisco equipment, however, I have experience with some systems, namely Windows and Linux, as well as some development practice as well.

You can find more about me on geek37.net.

Kevin Beaver — All right. Well, thanks again, guys. We certainly appreciate your time. And let's go ahead and jump into the meat of what we're gonna be talking about today. This is something that's really fresh on my mind. I've been touring around the country speaking at seminars on network security, mobile security, operating system security and including an event in Dallas just yesterday.

So, I'm rearing to go. I tell you, unless you've been living in a cave or under a rock in the past few months, you've had to have heard all of the breaches that have been taking place. I mean, a lot of security stuff has been happening. A lot of data breaches, a lot of hack attacks. Information is being stolen.

Systems are being compromised, just because. Things of that nature. So, a lot has been going on.

The Privacy Rights Clearinghouse over at PrivacyRights.org has been doing a study since February of 2005 and they've basically discovered that over 535 million sensitive records has been compromised due to security breaches and to me, I think that's really just the tip of the iceberg. You know, what about the stuff that goes unreported or what about the stuff that's undetected?

And, you know, with mobile devices becoming more and more prevalent. What is it? 162 million plus records have been compromised in mobile devices alone. And if you look at that chronology of data breaches you look at the types of organizations that are being compromised, you can see it's all over the map.

But I have largely seen SMBs, the small and medium sized businesses. These are my, you know, this my target market, the mid-market and up. And I'm seeing a lot of the security issues, a lot of the pains that they're up against and whatnot. So let's start throwing around some ideas and maybe we can share some insight with our listeners and provide them with some tidbits, some nuggets that they can take back to their office and put to use.

So, the first question that I want to throw out, guys, is what is unique about information security in SMBs? Who wants to go first?

Erik Goldoff This is Erik. I'll go ahead and jump in on that one. There's typically two things that are more unique in the SMB market. The first is lack of budget. And the second is lack of staff, which may be related to lack of budget. In the SMB market, I've run across law firms that have 12 to 20 satellite offices, but no permanent IT staff.

They don't have anybody on their own staff that's an IT ISO person, or an IT. So, basically, anything they know about security they either read in the news or you know, heard by the water fountain.

Kevin Beaver Right. Absolutely. Okay?

Andrew Baker Yeah. This is Andrew. I'm going to agree. The lack of budget is huge in that space, and also not thinking it applies to them. Right? People have this idea that security applies to you if you have valuable goods. We're not Fort Knox, so it doesn't apply to us. Or they think that when they hear security, they're thinking anti-virus and firewall.

So, not understanding the scope of security and not having the funding to and that's tied together right, cause obviously if you can afford the staff they might tell you otherwise and if you can't afford the staff then you're left with whatever preconceived notions you have.

Erik Goldoff Andrew's hitting on a good point.

Kevin Beaver Right. I think Andrew has are great point. Go ahead.

Erik Goldoff Andrew's hit on a good point with the understanding portion. And one of the big issues, you hear about data breaches. The other term used is the data is stolen, but in reality, the data is never stolen. Somebody breaks in, makes a copy of the data, and gets out. If somebody breaks in your home and steals your jewelry, you know it because the jewelry is gone.

But if you've got a business and somebody snuck in and copied your data and left, if you have no monitoring in place and no base lining in place, you may not know what's happened until it's way too late.

Kevin Beaver I think one of the biggest problems out there is that we often assume that these compromises are going to be visible.

You know, I think sometimes the media and Hollywood, they sort of play this stuff up and they think that. They make it look like firewalls are going to start smoking, and the routers are going to start smoking, and stuff like that. But it's not that obvious in so many cases. And getting to your point, Yeah.

Yeah. I mean, electronic information can be in more than one location at a time. So just because it's copied or stolen or whatever, it doesn't mean you're ever going to find out about it.

Fred Stuck I'd like to point out too that not in every case is something being stolen from you. It might be an attack on your clients. You know, for example, you know, there's sequel-injection attacks or cross-eyed scripting attacks where people break into your systems to try to break into your clients by injecting information into your web servers or into a database system that presents information to a web server.

And then when your clients go to your website, then they're attacked. Because they're loading a component that was put into your website that might redirect them to a, you know, a piece of Malware or something online. It's not always that you're the target. It could be, you know.

Kevin Beaver Right.

Fred Stuck Somebody that you're associated with.

Andrew Baker Subtraction by addition.

Kevin Beaver Yeah. I think there are so many issues. You know, every type of business, every type of organization, whether it's a corporation, a government agency, a school, or non-profit, I mean, we're all faced with the same types of things. But I do see unique challenges at the S ; B level, and it does tend to fall back on awareness at the management level.

The things that I'm seeing are the smaller businesses are being questioned by their customers or their business partners, and they're being forced to secure their environments because they do business with fortunately 500 companies and whatnot. So, they're getting sent these questionnaires, getting all these random phone calls from IT staff or compliant staff and whatnot.

So, I think that's a big part of what's driving security at the SMB level.

Andrew Baker Well, let me say this one thing though, Kevin. You said that they're being forced to secure their environments. I would say they're being forced to purchase security products. And very few people are giving people guidance on how to secure, right? If you look at the different frameworks

we have, they, the context of security is either the process and how you operate a security function.

How you harden a particular subsystem. PCI probably has some of the better guidance that tends towards security but no guidance puts it all together in a way that would allow you to say you're secure, it puts you, and we know the context of that statement anyway, but it puts it in a way that would allow you to say, "I've done all the checkpoints.

I've purchased the Firewall." and put it here. It has ACL. I have installed anti-virus. I have done these 18 things, and at the end of the day, those 18 things could still leave you vulnerable because it's not just owning them that makes you secure or more or increases your security posture.

Fred Stuck Great and to add to that. I mean just because you bought that firewall, if you don't configure the firewall securely, like Andrew mentioned ACLs. If you don't put the ACLs in, what is it protecting? If you don't make make sure that it's blocking certain traffic. That traffic's gonna get in and you're gonna get breached.

You know, you have to make sure you do due diligence and make sure that proper implementation of all the equipment. That's one of the simplest things that any company can do is just make sure that any equipment that they purchase if they implement them properly. Whether it's a Windows system, whether it's desktop, whether it's a firewall, a router, a switch, what have you, make sure you change the default password.

Make sure you, you know, turn off the things that aren't used that, you know, could be vulnerable to attack if you're not using them. Very simple things to do that generally, except for having the people on staff too, or having consultants that will do it for you, making sure that they're doing all these things.

Kevin Beaver Right and I think a big part of it is that people don't really know what they're up against. They don't really understand what's at risk and at the end of the day, you can't secure what you don't acknowledge. If you don't acknowledge that your firewall is not configured properly. If you don't acknowledge that your web application has SQL injection or cross- site scripting or maybe your anti-virus is not very effective on your desktops.

You know, if you don't acknowledge that stuff, you may have passed the compliance audit. You may have been able to go through this checklist and everything looks secure, you know. But it doesn't mean that your environment is truly secure.

Erik Goldoff One of the principles that I provide.

Fred Stuck Well, you're never going to achieve.

Erik Goldoff I'm sorry. Go ahead.

Fred Stuck Go ahead.

I was going to say is you can never achieve 100% security. It's cost ineffective.

Kevin Beaver True.

Fred Stuck You know.

Kevin Beaver True.

Fred Stuck And basically that's an illusion, you know, that we're 100% secure. You can only mitigate the risks that you perceive are the most likely to occur. Right.

Kevin Beaver Do you have something, Andrew?

Andrew Baker No. I think Erik.

Yeah. It was Erik, but I was about to say one of the principles that I try to educate my clients on is the concept of baselining. The only way you know when something abnormal is happening is by knowing what normal is. So.

Erik Goldoff Sure.

Andrew Baker Some people describe a virus attack is higher CPU and higher hard drive activity, but if you don't know what normal activity is you don't baseline, you really have no benchmark. So that kind of leads into one of the other questions that I had proposed and I get this all the time where people are

resistant to use open source and free software solutions, thinking that they're unsupported and second rate compared to the high priced stuff they can't afford.

I'll throw that question back out in a minute, but I say that to the end of, for the smaller budget clients, I recommend they set up something like MRTG or PRTG or Cacti. You can use SN MP mibs to look at your bandwidth out of your router. You can grab CPU cycle reports out of your servers just to get a baseline for what's going on.

Kevin Beaver Right. Now, I think one of the interesting things that I see is that people say, "Well, we don't have any technical staff." or "We don't have the budget to put these technologies in place." Well, you know, we have a firewall, we have anti-virus, and we back up our data and that's our, the extent of our security." But I think what a lot of people don't realize is that there are some free solutions that are already built into your operating system that you may not even know about, you may not be using to your advantage.

There's plenty of security components and security features built right into Windows XP for that matter. But all the way up to Vista and Windows 7, there are a lot of things that just sort of. They're sort of left undone. People aren't aware of, and again it goes back to the whole awareness thing. They don't know what they don't know.

Andrew Baker Well, it's part of that problem and I think this is something that small business owners don't get. If you look at what they're doing in every other area, if you look at their sales automation tools, if you look at their HR management tools, if you look at whatever tools it is, everything is coming down to the "push this button, get the common stuff you need done." And security is not like that.

Right, because security is dependent on your assets. I can't just give you a secure solution unless I am the one also providing all the assets for your solution. And, for your environment. So security is in a way like the difference between say the Mac OS and Linux where the Mac OS, Apple has customized the environment for you.

This is what you're getting. This is how it works. This is what it is, and you do the four things that they tell you you can do and you're happy about them.

In Linux, you could do 400 things and that can be daunting to some people who maybe only care about doing five things, and these other things go undone and are left in states that other people can use which is detrimental to them. So Security, nobody comes. This is why you still need a lot of consulting assistance, especially for small businesses who don't have their own staff or need staff augmented, to come and say, "Here's what I see", here's an assessment of what your environment is.

Therefore, this is what would help you increase or improve your security posture. And businesses that think there's an easy button from Staples that they can get to solve their problem will be mistaken.

Kevin Beaver And Andrew you bring up a good point, and this is something that has always been a pet peeve of mine at the SNB level is that there are consultants out there, systems integration firms that are selling these "network assessment services" where they come in, they assess the network, they figure out what you need, figure out how to make it better, and I actually have a lot of friends and colleagues that are doing these very things.

The problem is they're going in and doing the stuff and they're not really looking at security the way that it needs to be looked at. They may be looking at firewalls, maybe data backups, maybe anti-virus and that kind of stuff, but they're not digging in deeper like what you had mentioned. Okay, let's see, what exactly do you have on your systems?

What exactly needs to be protected? What's maybe not as high a priority? Where do we need to focus our efforts so, that is something that people need to be aware of that these network assessments aren't all that, you've just got to make sure you're looking in all the right areas.

Andrew Baker We're into second decade of the 21st century and we as security practitioners, as consultants, whatever, we have to continue to trumpet the idea, the concept, that security and technology must be wrapped in business processes for them to be useful.

And any services that provide you the technology or security outside of that are going to be less useful by default.

Kevin Beaver Right. Let me, let's move on to the next big question that I had, I want to get you guys' opinion on this. What do you think is the biggest security risk in any given SMB that people need to be thinking about?

Erik Goldoff Social engineering.

Kevin Beaver Social engineering? Can you expand on that a little bit?

Erik Goldoff Absolutely. There's a lot of ways that you can breach your company's data. You can go in through cross-eyed scripting. You can try do denial of service to get a buffer overflow, there's any number of ways to try and get in, but if you can get the people to let you in, they'll do the hardwork for you. A couple of examples, there's a whole series of fake AV Malware that's basically Ransomware and it looks like valid anti-Malware software, and they're trying to trick the user into clicking on something.

Once the user clicks on something, they're running the install. Another example is the end user license agreement for a lot of software including cracked software and some free software. Not all free software is great. And I'll kinda quote Mark Manase, give him credit for this. But a lot of people use the spousal install method, I don't know if you ever read the end user license agreement.

You go to install software and you just go okay, okay, okay, okay, okay until it leaves you alone.

Andrew Baker Yes, dear. Right?

Erik Goldoff Exactly. And what people are agreeing to and I've gotten some of these snippets on a previous demonstration that says, we will install software that monitors your surfing habits. We will collect data from your system to present you with better sales. So what they're telling you is first off they're gonna take data off your system. They're gonna monitor your habits and then they're gonna spam you, and you say okay.

Kevin Beaver It's funny you bring that up. You know, you think about that human gullibility. We see that in government gross. That's why government gets its measly hands and everything in our society because people are like, okay it's no big deal, I don't really care about what's going on right now and I can't really think long term about the consequences of this stuff.

So, yeah. Big problem.

Erik Goldoff It's becoming the biggest vector. There's email phishing attacks so you may be a member of the XYZ bank and XYZ bank's mass mailing company may have been breached. So now the bad guys have your email address and know you're a customer of XYZ they send you an email that looks like it's from XYZ that says click this link, it takes you to a site that looks like the XYZ Bank but says there's something wrong with your credential, please log in again.

You log in and you basically give them your banking credential. That's social engineering. It's not using the pry bar.

Kevin Beaver Right. Absolutely. Fred? Andrew? Anything?

Fred Stuck Yeah. My answer to this was going to be the human factor and social engineering as well. One thing that I would like to add is that, you know, for the small business that doesn't have the budget to develop their own, you know, security training awareness. There is a free one available from an organization called Infraguard.

It's a combination of business as well as the FBI, which I actually a member of and it's a security organization, not just IT security but pretty much everything. But they have an IT type security training at infraguardawareness.com and basically it goes in to things like what are the threats, employee behavior, passwords, social engineering, email use, a lot of the same kind of business topics that are in, you know, these custom, corporate security training awareness training type online sessions that companies are pushing out, and it's free.

You can create a free account, log in, take the courses and it would be great if, you know, if small businesses would require their users take it. They do have a test in certification. There is a nominal fee for that. However, you know just taking the course and, you know, having your employees take that course would definitely improve the human factor.

Andrew Baker Okay so I definitely agree with what Fred and Eric have said. The human factor is the case not only for small businesses, but for all businesses. Small businesses don't necessarily have different threat vectors than large businesses. They just have more awareness and resource problems. Right? So they have all of the problems, the security issues are coming at

them from all of the same places but they're either not paying attention to some of the places, don't think some of the places apply to them, can't afford to deal with the other places and are blissfully moving along.

They have money and targeted attacks against them are gonna be more successful because less people are watching the door, you know? What would happened to Sony Playstation network is what is happening to a lot of small businesses. They're completely, I wouldn't say they're unconcerned. They'd be concerned if they were aware.

They're just totally unaware of what's infiltrating their network and leaving steadily and we're huge losses because remember the SMB market refers to companies that could be making upwards of two, 20, 50, a 100 million dollars a year. So, that's not chump change.

Kevin Beaver I would say that any given business, any given network is one click away from compromise. You know, all it takes is one user being gullible, being stupid, having malicious intent. All it takes is one user to have your network infiltrated by clicking on some sort of Malware or going to some sort of malicious site that does whatever.

You know, we're talking about social engineering and the importance of user awareness and you know, making sure that our users are doing the right things, the thing is, you know we can have all the training, all the awareness programs in the world, we can be doing this on a consistent basis but we can't rely on it 100%. I've seen many organizations be very successful with their awareness programs, but you still can't rely on it 100%.

One particular scenario, I was doing some Internet response testing for one of my SMB clients and we left some of the some USB sticks laying around and a couple of people plugged those in and became "comprised or infected", just through our test application and I also sent out some e-mails with the companies letterhead with the logo and the company name misspelled.

It was really obvious. Had a lot a lot of typos in it, but I had a link to click on for the users to go to a specific page on my test machine just so I could see that they had loaded it up and interestingly, some of the very people who I thought were on top of security and who should have been

on top of security within the organization, including the HR manager, fell for this test.

It was pretty obvious, but it was kind of sad at the same time. So you can't have a false sense of security. You can't assume that just because you think you're doing all the right things with technology and training and audits or security assessments that you're going to be a hundred percent fool proof, because you're not.

Andrew Baker Listen, I worked in an environment where the people that had the most security issues were in development. Of the whole firm, we had one person in the business side and like five people in development that were killing us constantly in security.

Erik Goldoff I'd like to say that's uncommon.

Andrew Baker But then you'd be lying.

Erik Goldoff Exactly.

Kevin Beaver Right.

Andrew Baker But it also goes back to proper setup, where the developers want full local administrator control, so their machines get breached easier because instead of having least privilege to do the job they need to do, they've got more privilege than they should on the system and a little bit of a cock sure attitude.

Kevin Beaver Right, now, I still think that when it comes to SMB's, the biggest risk is not knowing what you don't know and assuming that you're not a target like what you guys said earlier and there's a quote by this German writer and philosopher, Johann Wolfgang Von Goethe, he said nothing is as terrible to see is ignorance in action and frankly that's what we see quite often, and I'm not trying to, you know, I'm not trying to say that this is anyone's fault. You know, it's just sort of a human issue that we're up against, and we're going to have to come up with some solutions to get the right people on board.

Andrew Baker Well, the problem is this, right? If you look at the last four or five years, technology's been ramping up. It's been on a steady ramp upstream. We know that. But most of the ramp up has been in the realm of connectivity.

Right? It's not just about getting a shiny, new this.It's you know. Apple's selling a gazillion iPods.

That's cool, but those people aren't really connected to each other. Okay. Apple's selling a gazillion iPhones. Those people are connected to each other. And a gazillion iPads. Now you're talking all sorts of connectivity and back into corporate system. What we have now is small businesses, which were traditionally Mom and Pop, they did what they were doing in the corner.

Everything was physical for them. Maybe they had a web site that was completely disconnected from who they were, it was just a banner over yonder.

Kevin Beaver But now they're getting in. They're starting to do their banking online. They're starting to do their bill payment there, they're doing ads there. They have a Facebook page.

They're doing these things online and online becomes a large part of what they're doing and they're ramping up and getting into this digital age much faster than their corporate maturity level. And so now they are easy targets. It's like shooting fish in a barrel. It's a ridiculously easy target and they're losing money and many cases they don't know it.

And if they run into someone who's not sufficiently greedy. All right. It's not going to bankrupt them in a single sitting. They're going to leak money. They're not going to know and this other person is going to be getting rich off of them, buying periodic things off of them. We're in a situation where the penalty for not understanding security is immense.

It's immense, and it's not like before. It's like wading naked through a field of poison ivy. You will get into a lot of trouble. It's going to be very uncomfortable.

Erik Goldoff The reality is crime is not new. Crime now is just taking advantage of the technology.

Andrew Baker Absolutely.

Erik Goldoff The turn of the last century, there were a lot of bank robberies. I think it was Dillenger, when asked why he was robbing banks, said, "That's where the money is."

Andrew Baker That's where the money is.

Erik Goldoff Right now you can get to the money through the ones and zeros.

Andrew Baker Yeah, without leaving your home and it, you know, it just changes the nature of robbing all these banks from an essential place.

Kevin Beaver Right.

Andrew Baker They have to understand that they're playing in the big leagues once they get connected to the web and in the big leagues people don't care who you are as long as you got money.

Erik Goldoff You know, these SMBs the same people that will lock the front door when they leave have no qualms about leaving passwords on Post-it notes on monitors, on having servers out in the open where cleaning crew or somebody posing as a cleaning crew could grab a hard drive out of it and walk away. So they don't understand the paradigm.

Andrew Baker No.

Erik Goldoff One of the interesting things that I see in my information security assessments that I do is that the risks or the vulnerabilities that I uncover are so predictable. I mean it's always missing patches, weak passwords, no hard drive encryption on laptops, you know, lack of policies, the no incident response plan.

And it's, I mean, it's the same practically everywhere I go and I think the problem is and I think this is sort of the issue with why maybe we're not maybe where we need to be SMB arena with security because I think people are overwhelmed. Business managers, even if they do understand IT little bit.

You start talking encryption, identity and access management log and event correlation and all these fancy technology terms, and they're just like, "Whoa. Hang on a second." They're overwhelmed. So they don't even,

they're not even putting their foot in the water, so to speak in addressing even the most basic issues.

I tell people if you address the low-hanging fruit, some of the silly, stupid stuff with security, you're going to be ninety, ninety five percent there, you know, you're going to be almost where you need to be your probably never going to be exactly where you need to be. You can't have a hundred percent security lock like with what one of you guys said a minute ago but just address the stupid, low hanging fruit and you're going to fix a lot of problems.

Andrew Baker Okay, so I'm gonna, I'm gonna take this opportunity to make a good point on what you just said here. The problem. That's not only a small business problem, right? It's a large businesses run into that same issue. The difference is large businesses have a greater margin of error, relative to a small business, okay.

A large business. Sony did not go out of business for all of the foolishness that they did and all of the money that they'll be paying for the breaches and the subsequent lawsuit.

Okay. They didn't go out of business, but if you're in a firm that's making 10 million a year and you run into that kind of problem where you lose records to the tune of, you know, a 100 million records. You're done. That's not even a question. You're done. Okay. So small businesses don't have that margin of error.

The other problem is that they get overwhelmed, when they get overwhelmed because sometimes I find that they didn't even know these things exist and you wonder how they couldn't, but when they get overwhelmed. It's because the people they're speaking to are primarily speaking to them about point solutions.

"Ah, you have problem X, buy this. You have problem Y, buy this." and it becomes this litany of tools and things that they're going to have to buy and implement with people that they don't have because of the money, that they have been thus far unwilling to spend or unable to spend.

Kevin Beaver Right.

Andrew Baker We, as a total industry, we have to look at security in a holistic way. Like we look at health in a holistic way. Right? You have to look at health in the complete eat right, sleep right drink water, get exercise. You can't be just one thing. You know, you don't look at somebody who's on death's door and you say, "Oh, That's because you didn't get enough sleep last night." It's gotta be a combination of things over time that as you do them that they're a habit that tend to better health.

Security is the same way.

Erik Goldoff I think it's, you know, it's just like with any issue, security, health, whatever, you know, you've got people who are really healthy, you've got business that are really secure. You have people who are pretty unhealthy. You've got businesses that are pretty unhealthy or pretty unsecure. It's the same concept. It's Murphy's Law.

There's never time to do it right, but there's always time to do it over, or have surgery, or take medicine for it, you know, we'll fix it later. So it is an interesting mindset.

Andrew Baker But when people start to drop like flies rapidly over health issues, you'll see more attention to health as you have in the past few years.

Likewise, in the past two years as we've seen all these breaches, I think we are going to start to see a little bit more attention to security earlier in the cycle.

Erik Goldoff Yeah. I'm going to change it up a little on you guys. Just brought an idea to mind that is part of the problem, and it may not be palatable to us as IT professionals. Part of the issue is the way in general IT professionals communicate with non-IT people. So, if you think back to the Charlie Brown cartoon, when he's listening to a teacher talk to him.

The teacher's talking and what he hears is whomp whomp whomp whomp.

Andrew Baker Whomp whomp whomp whomp.

Erik Goldoff Exactly. So, the IT professionals involved need to make sure that they are speaking in clear in common terms that can be comprehended without

talking down to the client. To make things very clear on what the issues are, what can be done, what should be done and what the risks are.

Kevin Beaver I think you hit it right on the head, Erik. That's exactly right. There are so many people in IT. There are so many egos, and so many people that think that they're God's gift to business in this industry and I have been there myself and before realized I couldn't be that way working for myself, you know, and you can't really get too far not being able to communicate with management and customers, so I think that's a great point and I'm glad you brought that up.

Erik Goldoff I've learned that one the hard way and over the years need to realize that IT is a tool for a business to create success, it is not the be all end all for the business.

Kevin Beaver Absolutely, Fred, anything to add?

Fred Stuck You know, how can I go with this. The issue at hand is a lot of times are resource issue. You know, small businesses like, you know, we've said earlier don't have the staff or the technical skill to take care of the infrastructure. Take care of the security whether it's from a networking systems standpoint or a holistic from a business continuity-type standpoint, you know, and I think that they have to make better decisions about the consultants and resources that they pull in-house even on temporary basis to take care of that infrastructure.

Make sure that, you know, hey, are you going to with the $40 an hour guy that doesn't know much and does this, you know, every once in a while at night, or are you going to go with the guy that is charging $200 an hour, but is going to get the job done and it's going to be, you know, properly installed all the security settings and everything are going to be mitigated.

You know, yes it does cost more to get it done right, but in the long run it's going to cost significantly more if a major issue occurs.

Andrew Baker Now, Fred, I am going to agree with you and simultaneously disagree with you.

Fred Stuck Well, I understand.

Andrew Baker Watch how this goes. The, I do agree with you that a lot of times people skimp and they go for cheap. They feel they can't afford it, and they try to

cut corners, or, you know, let's say if more fairly. They tried to do it as cost effectively as they believed they can.

Fred Stuck Right.

Andrew Baker And if they look and they see that there are twenty people on the market and some people are down at the lower end. They try to aim at the lower end, you know. It's also true that aiming at the high end doesn't automatically guarantee success. You got a lot of shysters.

Fred Stuck I agree that, I agree with you there. Definitely.

Andrew Baker Right, it is a hard for thing for them an, you know, just thinking through this we don't like we've been nice and fluid and free in the IT realm including information security. There may be, there may be room for some sort of standarization that can some sort of certification that can allow people to have confidence that the people that they are getting are qualified in some way and I know that certification is an automatic cure and I am not trying to propose that in this setting but there has to be some place that small businesses can can look and I think that is one of the roles the focus places is they provide a forum where people are vetted in some way that you can feel assured that the answers you're getting will lead you to the right solution, rather than you basically doing a Google search and taking people that look like the do security, because from a business user stand point how, do they know?

Okay, and now, and to tie that back to what we said earlier about the language. The language thing is interesting to it's sort. I don't disagree with either Kevin or Eric, I think that IT does get a reputation for being elitist at times and speaking a foreign language but I've also noticed in recent years that the business speaks something that's not quite English in English speaking countries and there is a lot of jargon and IT has to contend not only with the businesses' language and whatever barrier that represents between them.

But also with the media, because the media talks and sound bites and you know, we have all of this confusion about cloud because they run with it and marketing gets it and you've got everybody saying cloud on things that are not cloud, and the same thing with security, Malware everything is labeled the hackers.

Everybody is labeled a hacker. If they do anything remotely interesting with assessment penetration testing, breaking into things, this whole category of person that's called hacker and that confuses the issue for a lot of people and the overall access to information confuses a lot of people, and I think its good for places like Focus and I guess there need to be other classes of resource of this nature that can help people see. Here's what the real answer is. Here are some people that know what they're doing and are there to help your business and not just make money off you.

Kevin Beaver Right. We've got a couple more questions I wanted to make sure that we get to before we wrap up. So, let me throw this next one out here. Who should be responsible for security within an SMB when there is not a security department or a security manager. My general take on it is, you need to appoint someone.

If you don't have anyone, you need to hire them or you at least need to have an outside adviser that you pull in on a consulting type basis?

Andrew Baker Like outside legal council?

Kevin Beaver Yeah, exactly.

Andrew Baker I would say that a lot of times IT security starts in the IT team. All right? And to the extent that you call it IT security and not just information security or risk management, you can set yourself up for problems because you are making the scope a lot more narrow than it really needs to be. If you put security in the wrong place, I don't care who you put in charge of it, someone should have it as a role.

In a small company, a lot of people might be doing double roles. Your CFO might also be your HR person or your legal counsel or whatever. Make sure someone in the senior rank has security responsibility and that they delegate the operational part of it to some other person in the organization who has ample time to work on it, okay?

And make sure that they are reporting in not just on what tool I bought. But on what processes implemented. So the security person is going to interact a lot with HR, they are going to interact quite a bit with legal that you have on legal on staff. They're obviously gonna need funding for certain things and therefore they'll talk with finance and understand risk

but they need to be involved in every aspect of the business that has risk based on information.

And then you can have a successful implementation of information security at that organization.

Kevin Beaver Okay. Fred, anything?

Fred Stuck Yeah. I mean I agree with Andrew. It definitely has to be a higher level person in the organization, you know, security has to come from the top down. If, you know, the CEO or, you know, C level board of directors whatever, you know, you want to call them, if they're not focused on securing your organization the people below them aren't and also if, you know, you have a security manager that's put in place but doesn't have the authority to discipline somebody that violates that security because it's not pushed from the top down then they have no power and they can't secure the environment.

The real thing though is too is that everybody in the organization is responsible for the security of the entire organization and not just one person. Now, do I think that, you know, everybody's going to manage to secure themselves? No. I think you should have some, you know, structure to it. There should be somebody at the top that's responsible for, you know, developing the policies and procedures and maybe, you know, having some influence over the technology that's implemented, but you know, these policies and procedures need to be followed by everyone in the organization including the C-level people.

Andrew Baker Especially, the C-level people.

Fred Stuck Yeah, exactly.

Kevin Beaver Right. You know, you bring up an interesting point. I had not thought about this recently, but, you know, you have policies, you tell people they need to follow policies but in many cases, people are going to take the path of least resistance. They're not going to follow the policy, or they've got some other way of doing something and they're going to go around it.

What I had found is that you've got to step back and look at your IT processes and the way your business operates, and try to set your people up for success so they can automatically follow the policy rather than

having to remember to follow the policy. And you can often do that through technology.

And you know, business work flows through web applications or whatever. So, that's just a tidbit I thought I would throw out there, but do keep that in mind that you can't just expect people to follow policies across the board. You need to try to set them up for success as much as possible. Erik, did you have anything to add?

Erik Goldoff I was just going to, you know, enforce that everybody is responsible, so that was me saying thank you in the background. There does need to be leadership responsible for spear-heading. But every single person in an organization needs to be responsible for their portion of security whether that's, you know, keeping the door closed and not letting people into the data center or what the servers are or the phone room, not sharing passwords. Not, you know, going places they shouldn't using corporate computers, etc.

It's not one of these things. It's kind of like expecting the police to maintain security but leaving your door unlocked. It just, it's not going to work.

Fred Stuck I'd like to add another thing to what you said about, excuse me, the complexity of the policy, you know. If you make the policy that the people have to follow overly complex. They're not, they're going to get confused, and they're going to say "was I not supposed to do this, or was I supposed to do that?" and then they're going to make the decision themselves, and it's going to be possibly against the policy, and then it's going to be difficult for them to remember.

It's going to be difficult for them to follow, and the simpler the policy is, the better.

Kevin Beaver Right. You know you bring up a good point, that I tell people this is sort of one of my little, one of my little slides that I use in my presentation is that complexity is the enemy of security. Be it complexity.

Andrew Baker Absolutely.

Kevin Beaver Operational complexity, policy, procedure complexity, whatever, complexity is the enemy. If you make things convoluted and to the point where

people don't understand what to do, what they're up against, or whatever, it's certainly not going to help.

Okay. Let's. I want to take a couple minutes. I want each of you guys to take a couple of minutes and basically, trying to wrap up. Just try to sum up your main recommendations for SMBs, be it the executives at SMBs or maybe the people responsible for IT in the small and medium sized enterprises. Just take a couple minutes and give your final thoughts and closing remarks, so to speak.

Andrew, you want to go first?

Andrew Baker Okay, sure. Here are my thoughts on this. Security has to be tied to business goals. It is a business enabler if you do it correctly. It certainly protects the investments you're making elsewhere in the business. So, tie it to your business goals. Don't assume that you're not a target, okay? Because you are either because you have money or because most of the attacks are going to be scripted and they don't know that you don't have money until they've broken in.

Don't consider funding for security only in the context of infrastructure. In fact, practice saying information security rather than IT security and you'll be halfway there. Realize that you have tiny margin of error, relative to large companies. If you make mistakes that get you breached, you might not survive that.

The confidence of the organizations, of your clients, or the size of the loss might be too significant. And one part that we didn't say, teach principles of security, not just tasks, right? If people understand why they're doing what they're doing, if they understand how what they're doing ties to your overall objectives and it's practiced by everyone in the organization.

Then you'll, they'll be able to make the right decision in a new circumstance that your policy does not cover. But if it's just a matter of "do this thing", "do this task this way", even when it's illogical to do it that way because of a changed situation. They'll just follow the rules rather than try to think outside the box or worry about it.

So make sure you teach principles and not just tasks and make security a part of you overall business strategy and objectives.

Kevin Beaver Excellent. Thanks, Andrew. That's a great set of points. I especially like that last one, teach principles that tell people why. Erik, what about you?

Erik Goldoff I'll try not to repeat Andrew's good advice there. Kind of on the teach principles. It's good to illustrate others in your business that have had breaches and what the effect was. So, you know, hold up the picture of the bad guy to say, "Look what happened to them, don't let it happen to us." One of the critical things for your information security, if you want to protect an asset, you have to identify your asset.

So you need, within your business, I always advise them to identify what their assets are. It's possible to set up better barriers to the important assets to keep them more secure. I'd recommend strongly they join professional associations. Continuity planners, business continuity groups, PC user groups, anything within the field of IT, you bumped elbows with folks, find out what they're doing.

You get presentations from vendors where you get enough information to make your own decision as well as from the pure level to find out what's going on in other businesses which also leads to joining other professional associations based on your business and not on IT. Definitely the pure advice is a good one.

And the last thing, and I'm going to sound self-serving as a consultant but don't be afraid to bring a consultant in for a one or two hour consult just to get the ball rolling without buying any product. Just make sure it's a vendor neutral consult.

Fred Stuck Excellent.

Andrew Baker Well said.

Fred Stuck Right.

Kevin Beaver Yup. Absolutely. Okay, Fred.

Fred Stuck Basically, not to try to repeat everything that's been said already, This is just, awareness training. Whether it's using the free services like infaguardawareness.com, or other online services b7 talking openly with individuals in the organization about possibly of viruses, Malware, whatever, you know, security threat that's out there.

Whether it's automated, whether it's a directed attack, an internal attack. You know, talking about these things, making sure people are aware, conscious of it.

Just like you see on the news, you know about possible terrorist hacks, you know keep vigilant, keep an eye open you know, if you see a bag laying out, you know notify the police, notify you know, security personnel or something in that building, you know same kind of concept. Be aware of what's going on standard... how your computer is responding, you know if your computer all of a sudden responding slowly, and you know, you reboot it, and it's still responding slowly.

Let somebody know, maybe you have a virus, maybe you know, disconnect it from the network before. You know, it affects everyone. else. Keep an eye on these things. That's pretty much it.

Kevin Beaver Okay, thanks Fred and I'll leave I'll say this, I tell people you've got to know what you've got. You've got to understand how it's at risk, you've got to do something about it with technologies, the policies, plans and what not and then you refine and repeat over time. Know what you've got, understand how it's at risk, do something about and then refine and repeat that process over and over and over again so guys I want to thank you very much for being in this round table discussion today.

To those of you who have been listening, thank you so much for joining us. We hope that this has been beneficial. Feel free to reach out to us. You can find the event page again at Focus dot com slash event. And if you have any follow up questions, want to have any further discussion, please don't hesitate to reach out and hope everyone has a great day!

Kevin Beaver Thanks a bunch!

Andrew Baker Thank you very much. It was great.

Fred Stuck Thanks everybody. Have a good day.

FOCUS EXPERT

Andrew Baker
Director, Service Operations, SWN Communications Inc.
http://www.focus.com/profiles/andrew-baker/public

FOCUS EXPERT

Kevin Beaver
Independent Information Security Consultant, Author, Expert Witness and Professional Speaker, Principle Logic, LLC
http://www.focus.com/profiles/kevin-beaver/public

FOCUS EXPERT

Erik Goldoff
IT Systems & Security Consultant, Goldoff Consulting
http://www.focus.com/profiles/erik-goldoff/public

FOCUS EXPERT

Fred Stuck
Network Security Engineering, Sungard
http://www.focus.com/profiles/fred-stuck/public