SECURITY NOW!

Transcript of Episode #485

Expensive Lessons

Description: Leo and I discuss the week's major security events, including the Turla advanced persistent threat for backdoor for Linux. We then look closely at the very expensive consequences of the lax security measures employed by Target - and their massive late 2013 point-of-sale terminal breach - and Sony's whole-corporation network internal data dump and disclosure.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-485.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-485-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. There's lots of security news, including a Linux exploit you're going to want to know about. And then we'll get into the Sony hack. My goodness, the detail. We still don't know who did it or why, but Steve has some thoughts, coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 485, recorded December 9th, 2014: Expensive Lessons at Sony.

It's time for Security Now!, the show that covers your security, now. What? Huh? And - good name, eh?

Steve Gibson: Or soon.

Leo: Or soon. In this case we're going to look back a little bit. But Steve Gibson is here. He is our Explainer in Chief, the man at GRC.com, creator of the world's first antispyware tool and in fact kind of the discoverer of spyware in many respects. He's also the author of SpinRite. Hi, Steve.

Steve: Hey, Leo. Great to be with you. I had promised our listeners we were going to do a deep-dive episode. But I've seen so much email and Twitter traffic from people saying how are you not talking about Sony, that I'm like, we can't not talk about Sony. And I want to do more than just say, oh, it was bad, because that sort of misses the depth of the badness.

Leo: How bad it was.

Steve: Oh, my lord. I have, and I want to share, just I want to scan through the analysis of the files which have been released to date, which themselves is a small piece of the total 12-plus terabytes of data. And this is a situation where the guys who took it are having problems finding the diamonds in the rough because there's just too much. And so they've done things like - and the press has been confused because the press, you know, well, they're the press, you know, and we're about technology. So it's clear from what we're seeing that they've done things like scan for the word "password" in the filenames and then pulled all of the files from all of the employee workstations that had the word "password" in them and aggregated them and released them.

Leo: Actually, I do think that that was done by the bad guys.

Steve: That's what I said, yeah.

Leo: Yeah, yeah. The bad guys put out a Pastebin that they gave to the press, not to the public, but gave to the press. And they highlighted, like they put in a folder all the stuff they thought was really egregious.

Steve: Right. And so the problem is it's like they're being flooded with the wealth of what they have. And so every few days they've been releasing another 20GB or so. I mean, it varies depending upon what. So I want to talk about that. But then of course we have to talk about Sony's background and what could be done to prevent this. And there are some other little techie nuggets that have come out that I think are, like, just whimsical and hard to believe about this.

But the episode is titled - oh, anyway, so the point is, as we do, I want to cover the issue of Tor not being nearly anonymous as we had hoped and as many people wished it was. There was a very nice academic paper that came out that explained actually what a poor job it does. If anyone really applies their intention, it can be largely deanonymized. And of course we know that there are entities now out on the Internet with lots of funding that certainly have intention to deanonymize people on the Internet. So we will get to that when the news allows us to.

But I titled this podcast "Expensive Lessons" because I want to talk about two things in our main, you know, after we cover the more newsy stuff. And that is also some news that has arisen about Target, where it was like one year ago that they suffered that, what is it, 40 million of their customers' credits cards escaped, and 110 email addresses and other personal information. And of course we've got our regular news of stuff that happened during the week.

So we're going to talk about POODLE, which is an attack, of course, we recently discussed, which turns out is biting us yet again. That was the one that caused us to run away from SSLv3. Turns out that switching that off doesn't completely solve the problem. It can still affect some implementations of TLS. There is something we've discovered, an advanced persistent threat backdoor on Linux for the first time, which - or prominently for the first time. Judge Posner, whom we've talked about through the years, who's a pretty well respected U.S. District, I think he's Seventh Circuit Court judge...

Leo: Yeah, yeah.

Steve: ...said some scary things. And Cory Doctorow was just wonderful in response. And we have some miscellaneous stuff, and then we'll get into talking about Target and Sony.

Leo: I want to say Posner was the judge in the Microsoft case; wasn't he?

Steve: For some reason his name is so...

Leo: His name is so familiar.

Steve: So familiar, yeah.

Leo: Yeah. But I can't place it. But, yeah.

Steve: So it turns out that the POODLE attack is not completely mitigated as we had hoped by the frantic disabling of SSLv3. Just to remind our listeners, because we've covered so much territory on this because there's so much going on, the problem - the POODLE attack was the result of the fact that the SSL standard defined the two operations which must be performed, that is, authenticating the data and encrypting the data backwards. In SSL, they authenticate first and then encrypt, which means that, when you are undoing that, when you're wanting to turn the information back into plaintext, you reverse that process. You decrypt first, then you authenticate. Had it been done in the proper direction, the proper sequence, the first thing you would do is authenticate. And if you were trying to play any games, that would fail, and it would just be over. This whole exploit would never have happened.

But because you're decrypting first - and what POODLE uses is block ciphers. Unfortunately, the stream ciphers like RC4 have been pretty much discredited. No one thinks they're sufficiently secure, a stream cipher meaning that you're able to encrypt individual bits at a time. In a block cipher, because the underlying crypto system itself takes a block of some number of bits, typically 128, so that's 16 bytes, it takes 16 bytes at a time and, under the influence of a key, translates that entire set of 128 bits to a different 128 bits. Well, that means that you always have to give it multiples of 128 bits or 16 bytes. But if the data you're wanting to encrypt doesn't fall on an exact even multiple, then you have to come up with some way to pad that data out to an even multiple in order to encrypt it.

So therein lies the problem is that SSL never specified what the padding had to be. It just said "padding" because the argument was, well, it doesn't matter because it's just superfluous anyway. So do whatever you want to. And some various schemes were created for creating the padding. Well, it's that laxness in the specification that some clever researchers figured out how to exploit.

So this wasn't happening in the wild, but it was discovered and went public that it was possible, meaning that people then could do it. And the attack would be you get some code in your browser that would make something like 4,096 queries. And that would give you a byte of header data, which is still a lot of work to do, but it's feasible. So, as our listeners will remember, we scrambled around throughout the industry and removed SSL3. This latest update of Firefox that we described and we discussed last week, I think it's v34, completely removes SSL. Chrome has deprecated it and is, a version or two from now, they've said they were going to remove it. Okay, so people are turning it off all over the place.

What just came out is that as many as 10% of the Internet sites, tending to be the major ones for a reason I'll explain in a second, have remained vulnerable. And the reason is that there are still, even when you turn off SSLv3, that means you're always going to be requiring TLS v1.0, 1.1, or 1.2, which is the three versions of TLS we have so far. And that, the TLS does rigidly specify what the padding data must be. It turns out that, probably due to the history, that is, TLS was - probably the code actually used to implement an implementation of, create an implementation of TLS was inherited from SSL because it's almost the same. It's just additions and tweaks here and there, and version numbers in the header and so forth.

It turns out that many instances of TLS do not check for the adherence to the specification of TLS that specifies exactly what the padding must be. The fact that they can no longer be played with by a hacker neuters the ability for POODLE to work, unless the stack that you're trying to probe doesn't check on the server side. It turns out that, right now, today, 10% of the Internet sites don't check. And they tend to be the larger ones because they are those sites which are behind sort of big iron load balancers which themselves terminate the SSL or TLS connections.

So there's a company called F5 that makes one of the more popular frontends, so the idea being that behind this box are a whole bunch of servers. And this is the first box you come to when your fiber optic comes off the backbone through a router to this thing. So it's all your traffic. But it actually has your SSL certificate or TLS certificate, your website's security certificate, and it's got SSL/TLS security acceleration hardware, good random number generators, everything it should have except its code, its TLS code didn't get changed when we rifled through the whole industry. It may have had SSL3 disabled in it. But it turns out that, because it's an appliance, it didn't get the same OS updates as everybody else.

And I don't mean to pick on F5. There's also one called A10 which is a different manufacturer and company, same problem. Neither of them are checking, when they receive incoming traffic under the TLS protocol, for the padding adhering to the TLS specification. So POODLE still works against them. The companies have been notified. F5 already has an update, which I'm sure they're pushing out to their customers quickly. So anyway, that's - it hit the news because it just came out. I see in fact Adam Langley blogged about it 12/8, which is yesterday. So that's just happened. Again, probably not, you know, it's not the end of the world. The instances where this is a problem are being found, and it looks like it's a few major instances where they're not OS-based TLS stacks, but rather turnkey hardware frontend stuff.

The other piece of interesting news is - it's called Turla, T-U-R-L-A. I couldn't ever find where the name came from. Everyone just sort of started using it. It is an advanced persistent threat, an APT, targeting Linux in an interesting backdoor technology that I'll get to in a second. It turns out that it's part of another state-sponsored major espionage malware suite, but it doesn't look like it's our state this time. It looks like it's Russia. We know that the programmers work nine-to-five hours, which sort of - and that's from timestamps in the various modules of code that have been found. Nothing seems to happen on the weekends. They're home playing with the kids. And they seem to be in

UTC+4 is the time zone that they're in.

Instances of, okay, I've jumped over the part where I should say that it is at least six years old. Pieces of the Windows version - because this has always, up until now, been a Windows-only malware. So the presumption is a Linux backdoor module was added to extend its breadth as an add-on to this advanced persistent threat that's been around for at least six years. It was being called - Kaspersky and Symantec had it on their radar for a while. And it was being called Uroburos?

Leo: Uroburos.

Steve: Uroburos.

Leo: Uroburos is the snake that eats its own tail.

Steve: Yes. And in fact also known as the Snake. And people who can't pronounce strange words...

Leo: It's a strange word.

Steve: ...prefer calling it Snake.

Leo: Yeah.

Steve: So this thing has been Windows 16 and 32-bit - I'm sorry, 32 and 64 bits only. It was spotted 32 times in the Ukraine since 2010, 11 times in Lithuania, four times in the U.K., and then a handful of times in the U.S., Belgium, Georgia, Romania, Hungary, and Italy. So sort of more of a Western and Western-aligned feel than, for example, the other major state-sponsored discoveries that we've been talking about, which seem more like they're from us aimed in the other direction. This stuff sort of looks like it's coming at us.

Leo: Well, you saw that not only the Russians but the Koreans have this elite core of military - the North Koreans, military hackers.

Steve: A huge number. Wasn't it, like, 1,500 of them?

Leo: 1,800 in the Section 121 group. And they're well maintained, trained from youth. So every - I would bet every state has at least some elite core of hackers.

Steve: When we look at what this stuff can do, I mean, we did a full coverage of it two weeks ago, it is frightening. I mean, it's, like, it's no longer science fiction, although, I mean, it feels like we're talking about science fiction. But what we're talking about is, as we have said, and of course we will be talking about this when we discuss Sony here in a minute, security is alarmingly porous. And the more pressure you put on the attack surface, the more opportunity you can find to get in. In this case, the Windows components, which have traditionally been used, have used several known zero-day exploits to get in. They've also attempted to get in using long-since-patched exploits for Windows.

But also this system sets up a very - an extreme array of watering hole attacks. So they set up fake websites where they have, for example, videos that they lure their targets to through phishing mail that say, oh, you don't have the latest version of Flash. Click here to update your version of Flash. And of course what you're actually doing is downloading the malware into your machine. So these are highly, you know, very much like the state-sponsored attacks. This thing is meant to be super stealth, to stay under the radar for a long period of time, and to be aimed at specific targets in order to get into their networks.

So what happened is just in the last couple days, a couple samples of some Linux code were posted to the malware testing sites. And that tripped some of the alarms of the companies that have been monitoring this stuff for a while. What was found was a new Linux offshoot of this. So for six years it's been Windows-only. Now, this is based on, and this is what this Turla name, T-U-R-L-A, is referring to, based on actually a 14-year-old open source Linux malware, cd00r, which was then extended and modified. But in looking closely at it, they've seen pieces that are very familiar and old. So this stuff has been reused and recycled.

It is big because it is static. It's compiled from C and C++. It's an ELF executable with the symbols stripped from it to make it a little less easy to reverse-engineer. But whereas most code is - it's called "dynamically linked." Famously, Windows is DLLs, dynamically linked libraries - the idea being that you can assume a bunch of things that you need will be present on the system where you're running. And, if not, you can tell the person running the system, please update your GNU C library, or we need to have OpenSSL or libpcap installed. Well, in this case, this thing needs those modules, but it can't ask the victim to install them, so they're statically linked into it, making this thing 800-plus K in size. So it's a big blob that gets into your system.

What's interesting about this is it does use an older version of OpenSSL that is bound into it, v0.9.6, which is actually quite old because 0.9.8 has been current for a long time over in the 0.9 track. And it uses the libpcap network capture library in order to monitor the traffic on the victim's computer. Significantly, though, it does not require elevated privileges to run, which is unlike many of these things, where it's got to be run as root or admin in order to get the hooks that it needs in. In this case, a non-privileged user who runs this by mistake, who's, like, tricked into clicking on something to download this, is all the privilege this thing needs. No root needed. And it has some stealth capabilities. It disappears from the system, even though it's still running, so it won't show up when someone looks to see what processes they've got running.

And the way it works is interesting, and it gives us some clue as to what kind of machines it would be installed in. It monitors all incoming network traffic using its pcap interface in order to see what's coming in. If it sees a particular pattern of bytes in the header of a TCP packet - and, for example, in the case of the TCP packet, it's a specific ACK number. We've talked about the TCP protocol years gone by. The ACK is a 32-bit value which essentially acknowledges, thus the word, or the abbreviation "ACK," it acknowledges the highest numbered byte that has been received from the sender so far over the TCP connection. And so it will tend to jump by the number of bytes in sets of packets that it receives at a time. It doesn't respond to every single one. And packets typically have, what, 1,500 bytes or so. So it's going to be jumping through this 32-byte number space.

But if a specific TCP packet arrives with essentially what is - it's called a "magic cookie value," a key, or a UDP packet with - similarly, UDP doesn't have an acknowledgment, but it does have other stuff in the header. So if there's a match on either specific TCP or UDP data, this thing - oh, and it's using a raw socket in order to be able to monitor everything coming in. This thing creates a standard communications socket and opens an outbound connection to the IP address from which that special magic packet was received and connects it to a terminal session and awaits commands. So it is a stealth Linux persistent backdoor which - and what this tells us is, this means that it's not going to be useful on some Linux machine on an Intranet or in the back room somewhere. It's going to have to be a machine like a server which is Internet-facing such that public packets are able to get to it unmodified because, for example, if it were behind one of these F5 boxes that is doing frontend filtering, the F5 box terminates the connection. And then, essentially working like a proxy, it opens another connection.

So that's a perfect example of something that would prevent the raw incoming data from actually reaching the server. But so it has to have access to the public-facing Internet. And when then the bad guys know that they've managed to get this - they've infiltrated some organization, a company, a government, offices, wherever they're trying to get in, and that organization has some sort of public-facing server. It could be email, for example. It could be web. It just doesn't really matter that much. They then, when they want to execute whatever, basically whatever commands they want to on that machine, they just - they send it a magic packet containing this data. And then they will note that, within a second, an incoming connection from that victim IP is asking to open a connection. They accept that connection, and they're looking at a command window to that machine in that organization. And this has been found operating in the wild.

Leo: Oh, it's a zero-day.

Steve: Well, it's not itself a vulnerability. It appears to be an extension to this existing advanced persistent threat malware, which itself is about six years old, but we've only just run across this.

Leo: Yeah, guess you can't call it a zero-day if it's six years old.

Steve: Well, it's a new component of this whole attack platform. And what we're seeing in these advanced persistent threats is they obtain a foothold or a beachhead in the victim network; and, over time, they'll browse around. They'll see what's in your network. And it may well be that they get in via Windows through an exploit, through a phishing attack where they get an employee to go to a fraudulent website because it's something that they've already determined the employee would want to do, lure them there. The employee downloads something in Windows. But then once they're - and so that gives them their Windows position.

But then they look around and go, oh, look, this organization has Linux servers, like Linux-based web servers. So then they will use their Windows-based foothold to download this Linux malware and then install that through the Intranet into the Linux server. And that gives them another access into this corporation through the public server. And it might be something, for example, that people are less likely to check. They might have a Linux server in the closet where they're not backing it up frantically, or it's not having antivirus stuff scanned on it the way their Windows-based user workstations are. So it gives them a very potentially potent additional foothold into the organization.

So our friend, whose name is so familiar to us both, Judge Richard Posner....

Leo: Oh, I should have looked it up, yeah, yeah.

Steve: ...with the Seventh Circuit Court. He was speaking at, just recently, I think it was last Thursday, at the Georgetown Law Cybercrime Conference. And among other things he said: "It should be illegal to make phones the government cannot search."

Leo: [Frustrated sound]

Steve: I know. I know. He said also, if the NSA wants to vacuum...

Leo: What is the legal justification for that? I'd really like to know.

Steve: I know. "If the NSA wants to vacuum all the trillions of bits of information that are crawling through the electronic worldwide networks, I think that's fine," he said.

Leo: Yeah, why not?

Steve: And he went on to say, and this is the one that really got me, in fact Cory Doctorow was like, I mean, I'm sure he had to recover. Posner said: "Privacy is mainly about trying to improve your" - okay, this is Judge Posner, Seventh Circuit Court. "Privacy is mainly about trying to improve your social and business opportunities by concealing the sorts of bad activities that would cause other people not to want to deal with you."

Leo: Oh, that's an interesting statement. I mean, this guy's an intellectual. So he's thinking about stuff. He has said weird things before, including that he thinks that regulation of the buying and selling of children is a bad idea, that the free market should allow - so he's known for being outspoken. But I think a lot of this is kind of intellectual exercise. I hope.

Steve: Ah, well, maybe that was the, I mean, Cory did not take this lying down. There's a link here, a BoingBoing.net link in the show notes. And, by the way, I'm now including the link to the show notes with my communication every week to your guys, Leo, so that they can put that in the podcast feed so that everyone's able to get it more easily.

Leo: Yeah. The show site, which is TWiT.tv/sn, each episode should have these links.

Steve: Right. And from now on they will. Anyway, Cory wrote: "Posner conflates secrecy with privacy, another nonsense." He says, Cory says: "Your parents did something un-secret to make you, but I'm willing to bet that Posner doesn't want his own non-secret, baby-making activity to be recorded and viewed by strangers."

Leo: There you go. He might, though. You don't know.

Steve: Secrecy versus privacy.

Leo: He was - the reason we connected him with the Microsoft case, he was the private mediator brought in, agreed to by both the Department of Justice and Microsoft, at the end of that case.

Steve: Ah, okay. Okay.

Leo: So he was the guy who was kind of responsible for enforcing the antitrust judgment.

Steve: Right. Makes sense.

Leo: You know, he's an interesting fellow.

Steve: Yeah. I was sorry you were not with me last week because the previous...

Leo: So was I. And by the way, thanks to Mike for filling in. I really appreciate it, yeah.

Steve: Yes, yeah. The previous day you and Sarah had a great time talking about one of the things you and I have near and dear to our heart, which is Oddworld.

Leo: Ah. You love Oddworld, too?

Steve: Yes. Yes.

Leo: You don't play videogames anymore, do you?

Steve: Actually, no. And I really even didn't then. But that special series was so amazing that my company knew that pretty much once a year, when a new Abe or Munch title would come out, I'd be gone for a couple weeks. They just - that's like, okay, well, we'll see Steve when he's done because...

Leo: Love them. Love them.

Steve: Oh, my goodness. And so, and I listened to you talking about how you and Henry used to play it.

Leo: Yeah.

Steve: And I did, last week, even though Mike was like, huh? What? Odd what?

Leo: Oddworld? Abe's Oddysee? What are you talking about?

Steve: "Mike, I was planning to have Leo, but I'll just wing it without you." But, so, yeah. So what I learned is that what they've done is there is a new remake of the original 2.5D scroller called New 'n' Tasty. And this is thanks to you and Sarah talking about it because I was just curious, and I went back to Oddworld Inhabitants, where I hadn't been for years, because - and I completely agree with you. Trying to play Stranger's Wrath on a pad without really good controls would be just difficult. I guess, you know, kids do it somehow. But anyway, I won't drag our listeners through it all again because I discussed it at length last week. But I did want to mention to you, since you're a fellow Abe lover, that New 'n' Tasty is out on the PS4, with the other platforms coming soon.

Leo: Yeah.

Steve: So they will be making it available across the board.

Leo: I think the thing we liked about this, certainly I liked about it, was that it was just different. And so many videogames are the same that something that's unique...

Steve: Yeah, not only different, but clever. I mean, to have - for Abe, who is a floor polisher, to be working at Rupture Farms...

Leo: There's a sense of humor, isn't there. Yeah.

Steve: Yeah, there really was.

Leo: Now I might buy a PlayStation 4 just to play this. Although they say they're coming out on other platforms soon, too.

Steve: Yes. It will be out on all the various platforms.

Leo: Yeah. So the occasion for this was that Stranger's Wrath was reissued on the iPad. And I think it looks the same. It looks like the same game.

Steve: I think it is. And Stranger's Wrath, I explained last week that the history of this is that Lorne Lanning and his girlfriend Sherry [McKenna], I can't remember her last name, she happened to be, like, waiting for him to get home or something, hanging out in his living room, and on the coffee table she discovered a manuscript for a movie of this, that is, with Abe and Rupture Farms and all this, that Lorne had just been sort of playing with. And so she reads through it while she's waiting for him to get home. And then she's like, when he walks in the door, she's like, oh, my god. And she said, "Do you know what this is?" And he said, "Yeah, a manuscript I was sort of toying with." And she says, "No, this is our videogame." Because they were in San Luis Obispo. They were doing special effects and creative stuff, sort of as a satellite of Hollywood, as a producer of that stuff, wanting to develop some property of their own.

And so that launched them into, this concept launched them into videogames. And they didn't want to do a first-person shooter. They didn't want people dying and blood splattering and all that. And so, I mean, the worst that happens with Abe is that really evil creatures that you have no sympathy for whatsoever get ground up. But, you know...

Leo: You know, it's somewhat similar to the sense of humor of "Hitchhiker's Guide." And maybe that's why we like it.

Steve: Yes, yeah.

Leo: It's kind of a clever twist.

Steve: Yeah. Anyway, so I did recommend it. I commended it to our listeners. If you've got kids, oh, in fact, one of the things that Stranger's Wrath represented I was sort of sad to see that they didn't maintain. They were originally going to do a quintology. And Stranger's Wrath was sort of them succumbing to the first-person shooter pressure.

Leo: Yeah. Right.

Steve: And so they didn't shoot bombs, but they shot little furry creatures that were all teeth. So you'd, like, shoot it behind a wall, it would grab onto someone's butt, and they'd come running out from behind the wall, and then it would take them down. So anyway, fun stuff.

I did get - I saw as I was going through my stuff this morning a question from a Markus Sommer in Germany, who asked a question I see often, that I have answered before, but I just wanted to - since it's still being asked. He said: "Dear Steve, I've been a Security Now! listener for about six months, but I never bought a copy of SpinRite since I thought it to be a pure recovery tool." Oh, and that's why he probably hadn't heard it before, because he's only been listening for six months. He said: "However, you recently mentioned that it is in fact a preventive maintenance tool, not just recovery, so I was thinking about getting a copy.

"But there's a problem. Due to privacy concerns" - to which unfortunately Posner is not sympathetic - "I'm using full-disk encryption, TrueCrypt, on all of my hard drives. Since this will effectively prevent SpinRite from seeing the data structure on the hard disk drive, I assume that it will not work on my hard drives. Will I need to always decrypt the hard drive, then run SpinRite on it, then reencrypt it again? Or is there a way to work around this annoyance? Or might there be one in the next version of SpinRite," blah blah blah.

Leo: You are clearly, clearly new to this podcast, my friend.

Steve: "Love the podcast, and I'm already waiting for the next part of 'How the Internet Works.'" So, Markus, good news, run it absolutely as it is. You have a valid hard disk, regular partitions. They contain noise, but SpinRite doesn't care. The drive doesn't care what noise it's reading, and neither does SpinRite. It's all about helping and assuring that the drive will be able to read the noise or data, whatever that's there in the sectors. So yes, by all means, it runs with no problem on fully encrypted, full disk-encrypted drives.

Leo: Indeed it do. All right. Back to work, Steve.

Steve: Okay. So briefly, just to - this ran across my Twitter feed last week, and I thought, ooh, that's going to change a few things. We talked extensively one year ago, it was November through December that Target suffered that major breach. Boy, it's been a year, Leo. Time is really flying.

Leo: And what a cruddy year it's been. Breach after breach.

Steve: Ah, it's been a busy one. So to refresh, 40 million Target customer credit cards were compromised, meaning that 40 million of them had to report to their credit card company, or their credit card company informed them your card may be vulnerable, we're going to replace it. Which is really expensive. I think I saw the number $800 million. Maybe it was $400 million. It was a lot of money that that breach was believed to cost the credit card companies. And in addition, as many as a 110 million people may have had their personal information such as email addresses and phone numbers stolen.

Well, not surprisingly, that resulted in a landslide of lawsuits filed against Target. And at the time there was some concern that Target should have known. And therein lies the reason why they're probably in trouble, because a strong case can be made that Target was negligent in ignoring warnings that they were receiving.

Of all of the landslide of lawsuits, they were consolidated into just two: one lawsuit for consumers; one lawsuit for all the banks. So they all got together and said, okay, we're going to consolidate our complaint into a single suit. Target's lawyer argued, as they always have before, and as all other retailers always had, that they're under no contractual obligation, and that they have no obligation to the banks specifically because a third-party firm handles all of their credit and debit card payments. And so the Target attorney asked for the suit to be dismissed.

So the big news is a St. Paul, Minnesota judge, and I saw his name here somewhere - oh, Paul Magnuson. He ruled that Target's behavior "played a key role in allowing the harm to occur." He said: "Imposing a duty on Target in this case will aid Minnesota's policy of punishing companies that do not secure consumers' credit and debit card information." Even though "the third-party hackers' activities are what caused the harm, Target played a key role in allowing the harm to occur."

So this ruling is one of the first court decisions to clarify the legal confusion between retailers and banks and who's responsible in these data breaches because, in the past, as we know, banks have often been left with the financial burden of a hacking and responsible themselves for replacing the stolen cards. Oh, and here's where I had - I knew it was in my note here. The cost of replacing stolen cards from Target's breach alone is roughly $400 million.

So in my notes I wrote the Target ruling makes clear that banks have a right to go after merchants if they can provide evidence that the merchant may have been negligent in securing its systems. And at the time of its breach last year, Target had installed a $1.6 million advanced breach detection technology from the company FireEye. And we talked about it at the time. According to several people who were briefed on its internal investigation, who spoke under the condition of anonymity, the technology, this FireEye technology did sound alarms that Target ignored until the hackers had already made off with credit card and debit card information for those 40 million customers and the personal information of 110 [million] others. So this doesn't mean that the game is over yet. This just means that the judge has said, nah, we're not going to let you dismiss this, Target. We're going to go to trial.

Leo: Good.

Steve: And see how this proceeds.

Leo: Actually, I shouldn't - we shouldn't vote on this because it's really between the banks and Target. But one of the reasons this stuff persists is because...

Steve: They're indemnified.

Leo: Yeah, they're indemnified. We're indemnified, too. Retailers are indemnified...

Steve: We're indemnified.

Leo: And users are indemnified. The banks just absorb it all. I'm not in favor of the banks in any particular way, but this isn't ever going to get solved unless the people who are really responsible for the flaw have to fix it.

Steve: Right, right. Now, I did see an interesting piece from one of the SANS Institute editors, who read this a little differently. He said: "If the case is being made that, because Target had knowledge and ignored it, let's hope that the lesson that comes away is not to have knowledge." Because of course that is the...

Leo: Got it, right, be ignorant.

Steve: Exactly. We're not installing any detection software...

Leo: That's true. That's a good point.

Steve: ...because Target got hung because they knew and ignored it. And someone could easily feel that acting on this is too big a burden. Speaking of...

Leo: It is my understanding that the new law, the new chip-and-pin law, which goes into effect in the United States in October, we're going to replace our swipe-and-sign cards with chip-and-pin, puts the onus, or it puts the liability on whoever had the weakest technology.

Steve: That's what I remember reading also, yeah.

Leo: And that's obviously something the banks got in that law; right? But it does encourage - that's a good way to handle it because that encourages all the partners to have the best, most secure technology.

Steve: And it really does solve the problem because how many times have we said here that the problem with security is the weakest link is what gets attacked.

Leo: Right, right.

Steve: Well, so speaking of responsibility and not taking any action, even before this last couple weeks of revelations, how many breaches of Sony have we talked about in the past? I mean, the PlayStation has had breaches. I mean, Sony has historically had really poor security. And you would have to then hold them even more responsible for the depth of this catastrophe that they are now suffering. And it can only be called a catastrophe. We don't know yet for sure what the origin is, that is, whether - there are rumors that this is North Korea because of Kim Jong Un's unhappiness with the, what is it, "By Invitation" is the movie which is going to be coming out? Unfortunately...

Leo: "The Interview." "The Interview."

Steve: "The Interview." "The Interview." Exactly. But oddly, as a consequence of this, we know that the two main stars are each receiving $6.5 million because all the details of their contracts...

Leo: And James Franco gets $6,000 to drive himself to work.

Steve: Yeah.

Leo: I like that. There is a certain gossipy element to all of this, and I don't know if we should foster it.

Steve: Oh, that's what makes it so juicy. Oh, yeah, we have to, Leo. So, and Lizzy Caplan, I was a little disappointed, she's only getting $100,000 for her part.

Leo: What? A show.

Steve: No, for the movie.

Leo: Oh, in the movie.

Steve: Yeah.

Leo: Oh, she should get as much money as Sony has.

Steve: Well, yeah. Now we know exactly what that is, too.

Leo: A hundred thousand?

Steve: I know.

Leo: She's a super - she obviously did the deal before "Masters of Sex."

Steve: Probably did.

Leo: Yeah.

Steve: Yeah. And, boy, she's - anyway, you and I both like her a lot.

Leo: I hope she's getting a lot of money for "Masters of Sex."

Steve: I bet she is. And, what...

Leo: From now on she's going to make plenty of money.

Steve: Yeah, yeah.

Leo: But, you know, the question is, what is Korea's involvement in this? That's the interesting...

Steve: Well, and, yeah, okay.

Leo: We don't know, do we?

Steve: So one of the reasons I didn't talk about it last week or the week before is that, first of all, this is going to be providing juice for a year. I mean, the problem is the bad guys are having a ball trickling this out. And they've got so much content to disclose that there's no hurry. And I wanted to get a sense for it, too. So one of the things we have established is that a group whose initials are GOP, who goes by the Guardians of Peace, are clearly the source. We don't know much about them. We know that their English is not great. At one point, when they were disclosing something to the press, they said: "We've got great damage by Sony Pictures. The compensation for it, monetary compensation we want." Actually, they sound like Yoda.

Leo: [As Yoda] "Monetary compensation we want."

Steve: "Pay the damage, or Sony Pictures will be bombarded as a whole. You know us very well. We never wait long. You'd better behave wisely. From God's Apostles" - A-P-S-T-L-S. So, and similar messages like that in broken English and with words - there was also something that tried - it apparently pretended to be actually posted in Korean, but it looked like a machine translation was used to get it because actual Korean speakers said, no, the words are all, like, Yoda-ized.

So, okay. So here's - to say that it's bad, I think, misses the point. So I want to quickly just sort of scan through the contents of the data that has befallen the public from Sony's caverns so far because it gives - it's important, I think. As I was going through this, I was thinking, oh, my god, oh, my god. I mean, because it just, I mean, this actually did happen.

So on November 25th was the - and we now know that some small set of Sony's executives, two or three days before this, received an extortion email saying, pay up, or we're going to disclose a lot of information. And they ignored the email. No response came back to the Guardians of Peace. So November 25th, via a Pastebin link, torrent files were hosted on four sites in 26 parts as 25 1GB files, and then the sixth one, the fragment, was 894MB. They were also uploaded to filesharing giants Mega and Rapidgator, but the managers of those sites pulled them down. Those files contained information on 4,000 past and present Sony employees. And following this, a brief email dialogue that Risk Based Security, one of the many researchers following this, had with the GOP, the Guardians of Peace, stated that - the GOP stated that they had over 12TB of data, obtained from Sony's servers and workstations.

The next day, on the 26th, torrent links were published to Torrent Trackers containing the unreleased movies "Fury," which actually has now been released, but then three other ones: "Annie," due for release on the 19th of December; "Mr. Turner," due for release on the 19th of December; and "To Write Love on Her Arms," the title of a movie due for release on March 15, I'm sorry, March of 2015. And based on several torrent tracking sites, those three movies have been downloaded over 100,000 times. So they are loose on the Internet.

Monday before last, on December 1st, NBC News reported that the FBI was investigating the breach. Also the FBI sent out a flash alert a few days after that to a number of other high-profile companies, basically warning them to, like, watch their networks closely. One of the things we do know about the malware, and I'll talk about it in more detail in a second, is that it is able to jump through Windows shares, from one machine to another, through an Intranet. And this clearly helps to explain the depth of what was lost inside of Sony.

Leo: There's been so many stories about this. But I also saw that they thought it might have been an inside job because there were Sony logins to certain servers and so forth, so that maybe they were able to get that malware even deeper than they would have been with a spearphishing attack because they had some help from the inside.

Steve: Yeah, again, all we can do at this point is speculate.

Leo: Right. The FBI's not saying anything.

Steve: My sense is that this was ongoing for some time. I know that, for example, the malware was written for Sony. That is, in the malware were the names of 50 different Sony servers. So it knew what to look for. On the other hand, once you get in, if you can stay stealthed, you can poke around within a network. And clearly, in order for there to be this much data - 12TB. The other thing, Leo, that just cracks me up, and I've got this, later on I was going to talk about it, but Sony's own servers are providing the seeds for the torrents of their own data. So BitTorrent clients have been loaded on Sony servers. Then they're offering the torrents from Sony's own servers.

Leo: Wow. Oh, that - that's insult to injury. Holy cow.

Steve: So December 1st, another 24.87GB of data was leaked. Now, get a load of these numbers: 33,880 files in 4,864 folders, containing, just scanning through the data, 47,426 unique names with Social Security numbers. 15,232 Social Security numbers belonged to current or former Sony employees, 3,253 Social Security numbers appearing more than a hundred times throughout the files. And just among all this data, an example of employee data that was found is one file was in a directory structure - \HR\Benefits\Mayo Health\Mayo XEROX assessment feed - containing 402 Social Security numbers, internal email addresses, plaintext passwords, and employee names. So all of this confidential internal employee number and an additional 3,000 or more Social Security numbers, names, contact details, phone numbers, dates of birth, email addresses, employee benefits, workers' compensation details, retirement and termination plans, employees' previous work histories, executive salaries, medical plans, dental plans, their gender, their employee IDs, sales reports, copies of passport information and receipts for travel. It's just - oh, and account information to order customer jewelry from Tiffany & Co. via email. That was Monday before last.

Leo: Steve Gibson.

Steve: Okay. So I don't mean to belabor this, but some of these, I mean, our listeners will appreciate the horror of the fact that all of the security certificates for the servers at Sony, the file containing the security certificates has now been escaped to the public. Last Wednesday was a bigger blob. Oh, no, I'm sorry, smaller, because we're talking gigabytes, 1.8GB.

Leo: Oh, is that all?

Steve: The plaintext credential, the login credentials, about 500 of them, for all of Sony's servers and internal machines, IP addresses and data, with the security certificates, the users and services that those certificates are tied to. 121 FTP plaintext credentials, including the main Sony Pictures FTP server login. Just a huge number of password files which appear to be individual files, personal files, that Sony employees had on their own workstations, which they named "passwords," where they managed their own lists of passwords.

So it's not clear whether the malware attacked the backups of their workstations, which seems certainly possible, that is, all of this distributed workstation data is part of what was lost. I mean, it pretty much looks like everything was lost. So it may have been the workstations were being backed up to the servers, and the servers were sucked dry. But we also know that malware did get out onto the individual workstations because many of them had that weird skeleton screensaver that came up and scared everybody a couple weeks ago. And then there was also some drive wiping that was occurring. Data was removed, and then the drives were wiped behind them.

And I'm just going to scan through here for some other tidbits. Oh, on the 5th, last Friday, 100GB of compressed data which was titled the "Financial Data of Sony Pictures" - 22 individual files, making up three larger files, containing a set of newly released data. So in File 1, 30,916 individual files in just shy of 3,000 folders, making up 16.4GB of compressed data comprising...

Leo: That's a lot of compressed data.

Steve: Bank statements, bank account information including wire transfer swift codes. The financial year reports, financial year forecasts, budget reports, overhead reports, receipt and transaction account statements of computer hardware, vehicles, car accessories going back to '98. Internal information for Sony Pictures Releasing International portal, screenshots, walkthroughs, and other usage information.

File 2 had 89,800 files in more than 10,000 folders, 88.6GB compressed, had accounting information in the format of the Trintech, Inc., software, and then their licensing, their media, Sony's content licensing contracts with Access Digital, Amazon Europe, Amazon Japan, Clickplay Multimedia, Comcast, Eagle Eye, Gaia, Google, Media Vault, M-GO, Microsoft, PlayStation, Sena, Sony Visual Products, and too many other vendors to list, their actual licensing contracts in more than 90 files. 528 payrolls for Imageworks Canada with full staff names, contact numbers, and residential addresses. I mean, the actual data. All of this stuff has now been posted publicly on the Internet into torrents and in downloading sites. And files of federal income tax returns too numerous to count.

And then the third of these three files on just last Friday was, in another archive, 113,000 files in almost 40,000 folders containing incident reports of accidents of some sort with full names, incident locations, injuries, and positions held with Sony. Copies of employment contracts and agreements, passports, driver's license image scans, Social Security numbers and signatures.

And the last one I'm finished with is yesterday's drop, was four archives in two large files. The first .rar was corrupted and would not unpack. It was 3.5GB in size. We know that it was an Outlook mail spool. However, the second one did unpack. And that was titled APascal1.ost. Amy Pascal is the co-chairman of Sony Pictures Entertainment.

Leo: Oh, she's pissed. She's pissed now.

Steve: Her entire email spool, 5,000 emails. The most recent inbox email was dated November 23rd of 2014.

Leo: Oh, it's recent, wow.

Steve: So it is completely current, and it consists of emails to Sony Employee Relations, personal invoices, personal emails, includes talk and details about upcoming movies and current and closing business deals. So this is the private email correspondence of Sony Pictures Entertainment's co-chairman, Amy Pascal.

And they're just getting started, Leo. They have 12TB of this data. So this is, I mean, think about it, this is the entire internal operating data of Sony. Everything. I mean, payrolls, history, invoices, business plans, contracts. You know, Sylvester Stallone's Social Security number was, like, in among that stuff. You know, the pay stubs of all the actors that they've had on their movies. I mean, everything.

Leo: So we get it. Everything. So the question is - a couple of questions. First of all, I have to think that Sony is not the only company that this could happen to.

Steve: Oh, I completely agree.

Leo: And in fact, if you were targeted by sufficiently sophisticated hackers, there's probably few companies that would, I mean, is it possible to secure yourself against this kind of attack completely?

Steve: The problem is a mono culture and a mono network. That is to say, instead of being organized as small satellite networks that inherently have some containment, it's clear that a single attack event of some sort, at some time in the past, allowed someone to establish a foothold in Sony's network.

Leo: But you understand why it was that way. That's the easiest way to do business.

Steve: Yes.

Leo: You start siloing stuff, then it's a pain in the butt. You can't find out this. You can't find out that. You can't talk to this person. It makes sense.

Steve: Right, you can't get email directly from here to there.

Leo: And we should point out it is siloed in the respect that this is just Sony Pictures Entertainment. Sony is a much, much larger company. This is just one division of Sony, as big as it is. It's not like all of Sony was compromised, just SPE.

Steve: Right.

Leo: So it's siloed a little bit. It's just not - but you're not going to, I mean, I think about, okay, I think about our business here. Yeah, we use reasonable precautions. Our data's on QuickBooks. But I could easily see somebody getting into our internal networks.

Steve: Yeah.

Leo: And if somebody were determined enough, they probably could do it.

Steve: Yeah. I think, I mean, I'm trying to think of an analogy that works. And, I mean, if you switch to the real world, if someone came in the front door, heavily armed, with grenades and submachine guns, they could...

Leo: What are you going to do?

Steve: They could pretty much have whatever - they could have whatever they wanted. You know?

Leo: Right. Well, I need to go farther than that because - and this may be the real issue. Until the data era, security wasn't really, look, you lock your door, but anybody can get into your house.

Steve: We have windows. We have windows.

Leo: It doesn't really stop a determined attacker. It's more of a signal. And here's the barrier. Don't cross this because you'll be breaking the law. We have the law on our side. But it doesn't - if you're willing to break the law, a locked door is not a deterrent at all.

Steve: No. That's exactly right.

Leo: And so I think as we got into the digital era that same mentality persisted. Well, we've locked our doors. It's illegal to break in.

Steve: Yeah, you know, we put a password on our WiFi, even though it was our street address, so that we would be able to remember it.

Leo: What would be the burden of true security in a business? Not merely financial, but structural.

Steve: I would argue you can't do it in a sufficiently large and sprawling network where employees, by virtue of their jobs, have to have access. And unfortunately we are, you know, we've discussed the way firewall technology changed, where the original firewalls were open, and they blocked bad stuff coming in. And it was after it was painfully clear that that was wrong that firewalls were closed by default and then selectively opened ports where we did want to allow traffic.

The problem is we have, even in the computer that's in front of you and is in front of me, it is not a whitelisting computer. It is a blacklisting computer. That is to say, by default, it will run anything we ask it to. Now, there are whitelisting systems. And you can get them for your computers. The problem is they're a pain in the butt to use because you can't just download something and run it. You've got to get permission from IT, and they say no because their job is to say no. Their job is to prevent this from happening.

So my point is that, from the beginning, you know what I mean, from our mobile phones that are personal devices that people have in their pocket, and they walk into their organization, and they plug them in to charge them to a USB connection which is hooked into their computer. Now their phone, which who knows what's on it, has access to the USB port of their computer. And we know from the BadUSB exploits that it can do a lot of damage just from having access to a USB. So convenience, the real problem is that I think the only way you could have security is to have absolute mathematical certainty-level knowledge of every single component. And it's impossible today.

Leo: Right.

Steve: It's impossible.

Leo: I mean, we use LastPass Enterprise. We do all the prudent things. And I think we're just - so the only reason I bring that up is to caution people who are mocking and laughing and saying, oh, stupid Sony, as stupid as Sony is, as willing as I am to say that they have crap security, I'm not convinced that the same exact thing couldn't happen to most corporations.

Steve: I cannot conceive of securing Sony. I couldn't secure them. I could not secure them in a meaningful way.

Leo: They could have done much better. Putting a file on the desktop that says "passwords.txt" is a bad idea. They could have done better. But a determined attacker probably could get in anyway.

Steve: And, for example, I believe those are individual personal passwords files. So in an organization that size there were invariably a lot of people who were like, first of all, the fact that they had a passwords file means they had lots of different passwords. They weren't using a password manager that encrypted the data because they weren't that sophisticated.

Leo: We give everybody in the building here LastPass Enterprise. And I guarantee you there are some people with a file on their desktop in this building that says "passwords.txt."

Steve: Yeah, and they look up what the password is for that site. That's, I mean, so that's going to happen.

Leo: I never mentioned this, but we had an engineering director some time back who posted all of our company passwords, SFTP, all the secure stuff, on a public web server.

Steve: On purpose?

Leo: No. He just wasn't thinking.

Steve: Ooh. Ooh.

Leo: Yeah. He's not - he's not with us anymore. But that's - it's easy for that to happen is what I'm saying.

Steve: My point is it's almost probably impossible for it not to happen. You know, ivory tower guys can say, oh, yeah, you know, follow best practices. It's like, well, yes, but try to implement that across a company of 45,000 actual human beings who are not robots, who need to be able to access networks in other countries and actually do business. The problem is these systems are just fundamentally insecure. And the only thing I can think is that, if some kind of, as you said, stovepiping or compartmentalization were present so that, if somebody got into, I mean, so that there was a sense of not having all of the crown jewels on one big network in a set of interconnected servers that were able to see each other such that just getting a toehold allowed that to get pried into the crown jewels.

But think of what this means. Every, I mean, the security at Sony, within this division of Sony, is completely screwed. I mean, every single employee has to change every single one of their passwords, let alone every single server has to completely be rekeyed. I mean, it's just devastating. It just - it's just stunning what the impact...

Leo: Yeah, I'd hate to be the cleanup crew here, would be just...

Steve: Yeah, exactly, to remediate this kind of disaster. And then there's the reputation cost and the fact now that actors all know what each other makes, that that's now in the public. We're going to be seeing this data dribbling out for the next year, and it's just going to be hugely damaging, unfortunately, hugely damaging to Sony. And...

Leo: How long was PlayStation Live offline? Several months after their attack there. I mean, this isn't the...

Steve: Yeah.

Leo: This isn't Sony's first time to the rodeo.

Steve: No. And that's - some people have observed that one wonders what lessons, if any, they learned.

Leo: The lesson is don't get attacked. Don't anger bad guys. I think it's probably the same sentiments that brought down PlayStation Network are exhibited here.

Steve: Yeah, but, you know...

Leo: They alienated gamers. Don't ever alienate gamers. Bad.

Steve: True.

Leo: Oh, believe me.

Steve: Gamers have skills.

Leo: They have skills. Mad skills.

Steve: Yeah.

Leo: It's such an interesting story. And, you know, one last philosophical question, and I think a great one, from somebody in our chatroom, and I can't remember his name, somebody - sorry I didn't give you credit for this. But he said, how is it different, looking at this data that has been leaked from Sony, how is that different than looking at the naked pictures of celebrities that were released earlier?

Steve: Yes, I had the same thought while I was going through this. I was thinking, I mean, you actually have to just say no. You just have to say that this is data that is private. It is Sony's property. And no one should publish this. But, I mean, yesterday when I started doing this research, I saw one of the employment sheets for the "The Interview" where I saw the major actors' salaries on this. And there it was, on a website. So it is airing their dirty laundry.

And the person in the chatroom is exactly right. I mean, this is exactly the same. It should be - oh, and in fact one security researcher had the FBI come knocking at his door. He was not at home. His wife was. And she was, like, stunned, so she didn't even remember exactly what they said. But they were very intimidating. And what she remembered from their conversation was "illegal downloads." So what the FBI is now running around doing is trying to put their finger in the dike. They are trying to find the IP addresses of everybody who's downloading from the download sites and the torrents and trying to get the files back.

Leo: Oh, don't focus on that, FBI. You've got more important things to do than that. Really, that's the focus?

Steve: Yeah.

Leo: Let's try to catch the people. You can't put your finger in this dike. That is impossible. That's too bad that they're doing that.

Steve: So anyway, they are spending time that way. Well, they've got a lot of agents in...

Leo: They have plenty of things, plenty of time. By the way, it was Strengths in our chatroom who proposed that about the relationship between nude photos and the Sony data. And I think that one lesson is to maybe - it might be at this point bad mojo to have a little bit too much schadenfreude over this, that ask not for whom the bell tolls, my friend, because it could be you next.

Steve: Yup. The only thing, I mean, the only thing that I think works is keeping things small, keeping things simple. So if you had an IT person who was truly responsible for the security of a sub-network and the behavior of the employees and actually had authority, I mean, too often, I mean, IT people are complaining all the time that they get no respect; that they say, "We need to do this, we need to do this," it's like, what does that cost? Oh, well. It's like, "Okay, well, maybe we'll get around to that one of these days." But from my standpoint, complexity - we've said this often on the podcast - complexity is the enemy of security. And if you've got a gazillion employees on a common network, forget it. It's over before it begins. All it takes is any one of those people.

It's like the RSA, the devastating attack on RSA where one administrative assistant, and we know who she is, clicked a link, opened a PDF that contained an Excel spreadsheet, and the thing got into her machine, and now the bad guys were inside the RSA network. They stayed stealth, and they browsed around and found, like, watched traffic happening, and they just took their time. I mean, it is horrifying to think of something evil persistently living in your network. But if it's sufficiently large, if the network is, I just - I don't know how you prevent it from happening.

Leo: In some ways they're lucky that these guys went public with it. They could have just sat there forever and used this to their advantage. I mean, if you've compromised a network, the scarier prospect is that people didn't find out about it, and you just sat there and enjoyed.

Steve: And, you know, it really was stupid because they apparently, I mean, first of all, it does seem clear that English is not their first language. And to send an extortion letter saying we have data, pay us or else, I mean, no one knows how much money was being asked for. And, I mean, you would think, for example...

Leo: This could also be misdirection. If you're the North Korean government, then you might do that.

Steve: Could be.

Leo: It could be - there's some rumor going around that it's actually a Sony inside job, that it was a Sony employee who had an axe to grind. Of course the first thing you do is cover your tracks by pretending it was some hacker group.

Steve: Yeah.

Leo: We just don't know.

Steve: And talking like Yoda.

Leo: Yeah. We just don't know what the story is.

Steve: No, we don't.

Leo: But it's really terrifying.

Steve: Well, I think it's a wakeup call. I don't know that anything can change, though, from it. I mean, even in other boardrooms of other major companies, if the CIOs say to their COOs or CEOs, we're almost powerless to keep the same thing from happening, I mean, it's - you have to have access in order to function. And the bad guys can trade on the same access that the good guys have to have. It's like, I don't know how, I mean, I'd like to say there's an answer. But all we can really do is talk about the technology.

Leo: Right. That's our job. That's what we do.

Steve: Yeah.

Leo: Every Tuesday, 1:00 p.m. Pacific, 4:00 p.m. Eastern time, 2100 UTC, this guy here, Steve Gibson, explains it all. You'll find Steve at GRC.com. Next week, good lord willing and the creeks don't rise...

Steve: Q&A. Q&A.

Leo: ...we'll have a Q&A. And you can ask questions of Steve in two ways: one at the website, GRC.com/feedback; the other on this Twitter feed, @SGgrc. That also works. Steve pays attention to that.

Steve: I do.

Leo: You can go to GRC.com for a lot of other things, though. Of course SpinRite, the world's finest hard drive maintenance and recovery utility. All his freebies...

Steve: It's great on encrypted hard drives.

Leo: Yeah, it doesn't care. It doesn't know.

Steve: Nope.

Leo: You can also find 16Kb audio versions of this show, really nicely done transcriptions by Elaine Farris, who writes it all out longhand, at GRC.com. Now, at TWiT.tv/sn, that's our site, we have MP3 audio, high-quality audio, high-quality video. You can also find the show on every podcatcher out there because it's one of the longest running netcasts in the world, we're very happy to say, and we continue to do it each and every week. The bad guys are making sure to give us lots of material.

Steve: We're never running out.

Leo: Thanks, Steve. I'll see you next time.

Steve: Thanks, Leo.