

Featured Articles:

- Here's How to Fix Online Banking Fraud
- It's The Adversaries Who Are Advanced And Persistent
- New Data Show Most Breaches Come From External Sources
- Q&A: Bob Maley on Designing and Implementing a State-wide Security Program
- Anatomy of the RBS WorldPay Hack

Written by Threatpost Editors

Data Breaches Executive Summary

Data breaches have become a major threat to corporate networks in recent years, with hundreds of millions of lost records having exposed the personal and financial data of people worldwide. The threats come from all corners—hacker attacks, carelessness, insider theft—and imperil not just the privacy and security of users, but the integrity and reputation of the companies involved. This series shows the depth and breadth of the problem and the efforts of those involved to contain it.

Here's How to Fix Online Banking Fraud

Over the last few months, there's been quite a lot of news chatter around Banker Trojans emptying out online bank accounts of small businesses in the U.S. Today, I was reading one of such stories on Brian Krebs' site. After reading that story I came across another news item that described booting from an alternative media to experience safe internet banking.

That got me thinking again about an article I wrote quite some time ago. More specifically, I had to think of the portions on Man-in-the-Endpoint (or Browser as some prefer to call it) attacks. My opinion has not changed since then - MitE Banker Trojans already reached some sort of 'maximum sophistication' point back in 2007. This specific subset of Banker Trojans was -- and still is -- extremely sophisticated and will exploit per-bank specific vulnerabilities in the implementation of two-factor authentication.

So where are all these very sophisticated Banker Trojans? Well, they're very limited in number. Why? Because sophisticated malware is not needed to successfully attack the majority of banks. A lot of banks still don't employ two-factor authentication for making transactions. Or, when they do, it's a very weak form of two-factor authentication. Having some secret questions next to a password is not real two-factor authentication. Such protection is no match for most of the Banker Trojans/Spyware out there. Static responses - passwords, answers - should have been abandoned no later than 2007.

What frustrates me most is that there's an ultimate solution that will solve the online banking security problem to the greatest extent.

In short: Online banking requires multi-factor authentication. The authentication code needs to be received or generated on a device which is not connected to the device that's doing the transaction. Ideally, not only the transaction authorization code is generated dynamically but also the password for logging onto the banking site.

One thing to keep in mind here is that the cryptographic response algorithm needs to be different for logging on and approving transactions.

We should also realize that Trojans can (potentially) manipulate everything on your screen and in your traffic. The solution to this huge problem is actually quite simple. Make the receiving bank account number a part of the authentication process. Either send along the number with the SMS or use it as an (additional) challenge when using a token. The user knows where the money is supposed to go.

Some people argue that using the recipient's bank account number as a challenge, or any other code that will uniquely identify the recipient, doesn't solve the problem

as people may not pay attention. Well, when dealing with money, people should be paying attention. It's a silly excuse and does not take away that this is the only real solution to this problem.

Those banks that opted not to adopt my suggestions listed inconvenience as the main reason. This certainly seemed a much bigger thing with banks in America rather than Europe. For reasons unknown, American banks seem much more hesitant to potentially inconvenience their clients than those in Europe. Yet the clients I speak to in Europe are thrilled with the added security.

What we also need to keep in mind is that since 2006/2007, a lot has changed. The average sophistication of malware has gone up. Form grabbers, for example, are pretty much standard. In fact, we live in a day and age where Microsoft decided to pull a patch

because of problems which turned out to be caused by the extremely advanced TDSS rootkit.

What does this mean? This means that we need online systems in place that are resilient to such powerful malware. Using any other method other than using the recipient's bank account number there's no way even the best security expert in the world can say with full confidence that the transaction displayed on screen is actually going where it's supposed to go.

The state of online banking in some ways resembles that of the internet. For many banks, online banking was not directly designed with proper safety in mind. Convenience is the major driver. The internet was

built on very much the same principles. I'd argue that solving the online banking problem is an indefinitely easier task than fixing the fundamental weaknesses in the internet infrastructure.

So, let's start fixing the online banking problem. I think it's not nearly as hard as people may think it is. The necessary solution is out there and published. All it takes is for a number of clients to start speaking up and demand better security. Surely one bank will see the competitive advantage of offering better security. From there on other banks will follow. Losing significant amounts of money or a little added inconvenience which can be minimized? I know which one I'd pick.

** Roel Schouwenberg is a senior anti-virus researcher in Kaspersky Lab's Global Research & Analysis Team.*

It's The Adversaries Who Are Advanced And Persistent

There has been much talk recently about the "Advanced Persistent Threat." According to Richard Bejtlich [1] and others, the term originated with the US Air Force around 2006, which explains why Bejtlich and others with an Air Force pedigree, such as Mandiant founder Kevin Mandia, have made much of the term.

Recently has it begun to enter into more common use, particularly in the wake of the recent Google incident. Since that story broke, the term can definitely be seen scaling Mount Hype, with high probability of reaching the summit by the RSA Conference. This is, of course, why all those DLP banners were printed one-sided.

The Next Big Nail

Part of our concern is how much the term is likely prone to abuse. Those with a hammer to sell will undoubtedly see APT as The Next Big Nail. Not only does this promote the myth of the "easy button" in security, where a new tool, technology or product emerges to solve the latest headache, it also lumps APT into the FUD bucket of everything we fear we can neither understand nor see today. It doesn't help that the term itself plays to the U in FUD, particularly when tactics are neither advanced nor seemingly persistent. But this is part of the issue in our view: a good deal of the problem with security today is that we focus our



The advertisement features the Kaspersky logo at the top left. Below it, the text "Real-Time Deploy" is written in green, with "Protect" in large red letters in the center. To the right of "Protect" is "Manage Malware" in green, and "Expectations Protection" in smaller green text below it. A green banner at the bottom of the ad contains the text "Kaspersky Open Space Security". Below the banner, it says "Get Your Free Trial" and provides the URL "usa.kaspersky.com/downloads/".

attention on tactics, rather than what is behind them.

What we would prefer to consider, then, is the “Advanced Persistent Adversary,” since “threat” becomes all too easily confused with tactics.

This is not semantics, but it very well could be about Symantec - it is significant that McAfee came out and named the GOOG Thing, and fanned the flames of this new bonfire of mainstream APT-uttering. For example, in the blog post proffering the name Aurora to describe the wave of attacks in which Google found itself playing a starring role [2], McAfee defined APT thusly:

“The current bumper crop of malware is very sophisticated, highly targeted, and designed to infect, conceal access, siphon data or, even worse, modify data without detection. These highly customized attacks [are] known as ‘advanced persistent threats’ (APT).”

Clearly, McAfee avers that APT is a new form of, or state-of-the-art in, malware. That is precisely wrong.

Conflating Risk & Threat

This feeds right into another, larger issue in information security: that practitioners often confuse and conflate the terms they use to describe what they’re talking about. We’ve heard high-ranking security executives refer to specific viruses as “risks.” With mainstream use of “APT,” it becomes a “thing” which can be “solved”. By calling a specific threat like an exploit or a technique an “advanced and persistent” one, it makes it sound like a missile: something that must be controlled lest it proliferate. In fact, these exploits and techniques seem more like handguns - more agile, smaller, cheaper, easier to use and carry - and a whole lot more difficult and controversial to control.

If we allow vendors to say that the “threat” is the problem, then, “advanced persistent threat” is relegated, as it has been, to the people we have been paying to clean up what we have typically labeled “threats” [3]. Not only does this play into that “easy button” mentality (which is likely the worst possible way to address the advanced adversary) but also it often draws the focus away from a coordinated incident, and towards individual tactics that may be misleading, if they are detectable at all. It may well be that a specific tool used by the more adept adversary is not at all advanced, and may not appear to be persistent. In fact, if they’re any good at it, their activities will appear to be benign until it’s too late.

A Little Light Musing

To use a classical piano analogy, there are millions of people the world over who feel up to taking a crack at Beethoven’s “Für Elise” - including professional concert pianists. Relatively few, however, can do a competent job with the Hammerklavier sonata, one of the most difficult in the classical repertoire. But here’s the thing: those who can deliver the Hammerklavier can also handle “Für Elise.” The point is, they can call upon the right piece for the moment, regardless of the level of challenge.

The “threat” in APT isn’t about the tools used, or whether they’re common, or dated, or ridiculously simple. (Indeed, if you wanted to call upon a simple tactic as a red herring, why not if it suits the purpose?) It’s the adversary who shows virtuosity, the adversary who shows persistence.

Advanced, Persistent Adversary

The more advanced adversary demonstrates persistence, because it has a larger strategic goal than any individual exploit, or even any individual incident. And the adversary may have the resources to back not only expertise in tactics, but such things as fundamental research which can be called upon as the need arises.

This also helps shift the focus where it needs to be. We have been far too lax, for far too long, in the way we think about how to counter threats of any kind. Pieces and parts, this tactic or that, some new tool for every new emerging exploit, without considering that the adversary thinks far more strategically than we do.

We would hope that this also shifts thinking in the security market toward a more systematic approach to defense. For Pete’s sake, the rockyou.com breach alone ought to demonstrate that we’re still unable to build a decent foundation for our efforts, let alone ready ourselves for the more advanced, persistent adversary.

Things That Can Help

Many still-accepted approaches that are successful in producing revenue for security vendors will have little or no bearing on dealing with the advanced adversary, but there ARE things we can do to improve our current situation, which today we clearly do not.

Let’s think like the adversary and assess ourselves accordingly - and we’re not just talking about vulnerability scans. How do our companies appear to the

world on the Internet? How do our employees and business units communicate with the world, and how do our applications expose ourselves to the Internet at large? And how aware are we really about what goes on in our environment? Are we monitoring as widely and well as we could be? Are we making use of the information we collect and doing what amounts to pre-incident forensics on the data? If not, or if such techniques seem beyond our reach, where can we look for expertise that will help, and what does that need say about where security management needs to go in the future?"

It's high time we began setting our security goals to align with defense of what we hold dearest.

All too often we set our security goals to align with those of compliance with regulatory or industry rulesets.

One thing we believe will not help: more of the same. The advanced, persistent adversary has been here for some time [4]. Here's some time-worn advice that's been around for a while as well: there is no panacea, there's no magic bullet, there's no boxed solution ready for cash and carry.

While many rightly raise that the Google incident is the first time the issue has made the mainstream press, there's lots of experience out there on the user side, and we applaud experts like Richard Bejtlich, Mike Cloppert and others (like Will Gragido at Cassandra Security who's been writing about another, different way to describe this, Subversive, Multi-vector Threats, or his business partner John Pirc, who presented on many related issues at ToorCon 2009) who have come forward to share at least the anonymized takeaways of their work. As we went to Press, Andy Jaquith published similar thoughts at Forrester.

We need more experienced practitioners to come forward and share. As you read this, information security pros are sitting, wide-eyed, in banks, insurers, card processors, chemical firms, all kinds of industries, analyzing the latest - that is, today's - onslaught. Sharing our common experience makes us all stronger.

McAfee was right when it said that, "Everyone's threat model now needs to be adapted to the new reality..." Organizations sharing information with one another is one great way to speed our time to insight as we grapple with just what that new reality comprises.

* Scott Crawford is Research Director at Enterprise Manage-

ment Associates (EMA), a leading IT industry analyst and consulting firm based in Boulder, Colorado. The former head of information security for the Comprehensive Nuclear-Test-Ban Treaty Organization's International Data Centre in Vienna, Austria, Scott has been an IT professional in both the private and public sectors, with organizations including the University Corporation for Atmospheric Research and Emerson (Fortune #94 in 2009).

* Nick Selby is co-founder and Managing Director of Trident Risk Management, where he consults Fortune 1000 clients on information security, data protection, penetration testing and vulnerability and risk assessment. TRM also consults with government and law enforcement agencies on intelligence issues and tools. He was, in 2005, the founder of the Enterprise Security Practice at industry analyst firm The 451 Group, and is a Faculty Member at IANS. He is a regular contributor to FudSec and ThreatPost.

1. Bejtlich himself has massive experience in facing down all kinds of threats from advanced and persistent adversaries, in several distinguished roles. He has been raising awareness of these issues, as has Kevin Mandia, for several years

2. The use of the name itself confusing, because "Aurora" has been used for three years to describe an Internet-based attack against rotating generator equipment and was recently highly publicized in a controversial CBS 60 Minutes segment. Yes, McAfee had a reason to name it that, but that doesn't mean it should have. Nick's wife makes and sells tremendously good baked goods, but that does not mean she should call them "Oreo"s

3. And how's that working out for you, hmm?

4. Of course it is enough to make one physically ill to hear that MSFT had long known of the problem that caused GOOG so much angst. In fact, if you want to raise your blood pressure, consider just how long it took for McAfee and Symantec to begin to address APT - and now consider that they're trying to dominate the talking head space, issuing punditry and thought leadership around APT to sell, wait for it, anti-APT products. Thanks, guys!

New Data Show Most Breaches Come From External Sources

New data compiled by Verizon in an addendum to its Data Breach Investigations Report shows that the vast majority of reported and investigated data breaches

Spotlight Series

are the result of external incidents, not insider threats.

“Incidents that result in data compromise and that prompt disclosure or outside investigation are most likely to be perpetrated by external threat agents,” the report says.

The report, which is an update and expansion of Verizon’s annual Data Breach Investigations Report, takes a detailed look at the anatomy of data breaches and how and why they occur. The data that Verizon analyzes in the report is taken from the public data breaches that have been disclosed and investigated. So it does not include information on incidents that didn’t trigger a disclosure or were otherwise not made public.

But what the report does show, is that the data compiled by Verizon matches up very closely with slightly normalized data contained in the DataLoss Database, a massive collection of reported data breach incidents. In order to make the Data Loss Database information map more closely to that gathered by Verizon, the Verizon researchers removed incidents from the DataLoss DB that were the result of “lost assets, improper disposal and postal mail errors.”

The result is that Verizon’s data show that 73 percent of incidents are the result of external events, while the modified DataLossDB data shows that 79 percent of incidents came from external sources. That’s a remarkably similar result. But, as the Verizon researchers point out in the report, it’s not necessarily a conclusive one.

“The modified DataLossDB dataset nearly mirrors our own. We find this fascinating. The agreement between these large historical datasets increases our confidence in the following assertion: Incidents that result in data compromise and that prompt disclosure or outside investigation are most likely to be perpetrated by external threat agents. The assertion should be read carefully as it contains important qualifiers. Neither of these datasets contains unknown incidents. Neither contains undisclosed

incidents that were investigated internally. Perhaps such incidents differ in quality than those contained within our caseload and DataLossDB. Perhaps they don’t. Without data, neither hypothesis can be tested. We must manage according to what we know and then try to prepare for what we do not know. Table 5 represents a large sample of what we know,” the report says.

The data sets compiled by Verizon and the DataLossDB are quite different, due to the nature of the work each organization does. Verizon’s data leans much more toward attacks and malware infections, whereas the DataLossDB mostly comprises incidents that were the result of thefts or mistakes.



Q&A: Bob Maley on Designing and Implementing a State-wide Security Program

Dennis Fisher: Welcome to the Digital Underground podcast. This is the first episode in what's going to be a series of podcasts with CSOs from states around the country. We're going to be discussing the unique challenges of running an InfoSec program in the public sector and what lessons enterprise security staffs can learn from their counterparts in government. So my guest today is Bob Maley, the chief information security officer of the commonwealth of Pennsylvania. So Bob, welcome to the podcast.

Bob Maley: Thanks, glad to be here.

Dennis Fisher: Alright, so you and I had a discussion a couple of years ago and you were the first CISO of Pennsylvania when you took the job in 2005 I think and you were sort of starting from scratch. They really didn't have an information security program, at least sort of a united one at that time. So what was the state of things when you took the job in '05?

Bob Maley: Well back then given that most states typically are very distributed with their IT as well as their security and under the governor's administration here there's around 47 agencies, boards, and commissions and at that time most of those folks, the larger ones were doing things independently.



Kaspersky
edges out the
competition.

Cascadia Labs evaluates
the true capabilities of
endpoint security suites.

usa.kaspersky.com/threats/

The graphic features a bar chart with four bars of increasing height from left to right, with the tallest bar on the right. The text is positioned to the left of the chart.

There was no coordination and several years, I guess it was about a year and a half before I took the job that the commonwealth had been victim to several virus outbreaks where they experienced some significant outages and at that time the office of information technology decided to launch a lot of technical controls and consolidation of those types of controls like centralizing antivirus and they had put some things in place that they were ready to take a look at but there really was nothing there, for instance enterprise-wide intrusion detection and prevention in a host space, incident monitoring, incident reporting. So there were a lot of things that had been talked about but nothing had been done. There was no policy really. There was an older policy that was written about three or four years ago that really had become irrelevant. So it was kind of like a clean slate. I was able to come in and really start a program from scratch designed after where I felt we should be taking the commonwealth and it's worked out pretty good.

Dennis Fisher: So what were your top priorities when you came in? Did you have specific mandates from the higher ups as to what they wanted you to focus on?

Bob Maley: No, there were no mandates at all. Obviously other than the number one mandate and from the very beginning I put this into the security division's mantra, our reason for being, and that's protecting citizen data and whatever we had to do to make that happen is what we did.

Dennis Fisher: Okay so what were the things that you focused on, the first maybe three or four things when you got in saying you know what, we need to tackle this, this, and this?

Bob Maley: Well, like I said, there had been those technical programs that were under way and I had the luxury I think of being here as a consultant prior to taking the role and I was managing five, or I was the project manager for five of those technical controls.

So the first thing obviously was those things we were rolling out, those things we were beginning, we had to ensure that a) they were appropriate b) that they actually would produce the results that were intended and c) we had to make sure they were rolled out effectively on time and we did those under budget as well.

So that was the number one priority, to get those technical controls in place. The second thing that we undertook was looking at the security policy that we had and we had a policy that was written several years before and was really written with an operational slant. At the time there really weren't any connections between the needs of business. Even though we are government we are in business for the benefit of our citizens, services to our citizens, and our agencies all have specific business needs and that's a point that kind of got missed. So we had to go through that process and totally rewrite what was there, introduce new policy for areas where it was lacking, and then an ongoing process of making sure the policies that we were doing were kept up to date.

Dennis Fisher: Okay and you mentioned the sort of unique challenges of being in the government. It is a business as you said. You're not trying to waste money aside from what some people might think. But how much pressure is there in terms of budget because obviously the economic situation in the country is not great these days and everybody is sort of feeling the pinch. So how much has the economic climate affected what you're able to do internally?

Bob Maley: Well I think not a lot simply because we've developed our programs around the fact that budgets are tight even before the economic climate hit us. We're very, very cognizant of the security in the private sector. It's tough enough to get security elevated to a position where senior management, the stakeholders look at it as an investment in the bottom line of business as opposed to an expense and the worst security programs obviously are looked at by management as an expense.

Dennis Fisher: Yes.

Bob Maley: I was able to develop a marketing strategy that I think we overcame that early on. We did a lot of things that were more or less no budget that really produced significant results that allowed me to go and show that we do want to do this project and yes this project is going to have an initial cost to it but here are the ongoing benefits. Here how the citizens of Pennsylvania are going to get value out of what we do and by doing that I think we've put ourselves in a situation that when we do go for funding that I don't

have that significant challenge of well we don't even want to talk to you, you're not even allowed at the table because you're just an expense.

Dennis Fisher: Right.

Bob Maley: So I don't have that challenge. Now I do have the challenge that every other business unit has that we are competing for the same amount of funds and sometimes it is difficult but when we do our requests for funding, I don't use the fear, uncertainty, and doubt factors.

Dennis Fisher: Yes, yeah.

Bob Maley: We actually produce a very comprehensive business case analysis that shows what's the benefit and this may sound strange coming from government but what's the benefit to the bottom line and our bottom line here is we're not a profit obviously. We collect taxes. We do all those things that the government does that we all hate but we still have to do them and so we have to make sure that our business units, that they can accomplish those goals that have been set out for them by the governor, set out for them by the legislature, whatever goals they happen to have and we just make sure we can enable them to do those things securely without impeding their business processes and it's really resounded well throughout here and it's put me in a position of getting to implement programs is not as difficult as one might think.

Dennis Fisher: You made an interesting point, this thing about actually developing a business case for the programs that you want to implement in the coming year and I feel like maybe that's a mistake that some CSOs and even other security managers in private organizations make the mistake of maybe not doing that because they haven't had to in the past but they just kind of walk in there with a list of the current threats and how much more malware there is this year than last year and saying it's only going to get worse next year so I need more money next year.

Bob Maley: Right and it doesn't work. It doesn't fly because in private sector right now, all the vendors that we're dealing with, everybody's tight. Nobody's flush with cash.

Dennis Fisher: Yeah.

Spotlight Series

Bob Maley: And there are definitely competing folks within the organization. So if you're going to go in and try to sell these things by that fear, uncertainty, and doubt, unless you've really had a serious event that hit home, most people are going to go well it hasn't happened and okay you told us that last year and the year before and nothing's happened so why should we waste money on a program that we don't perceive as we need?

Dennis Fisher: Yeah and you can keep saying well it could happen.

Bob Maley: Right.

Dennis Fisher: But that's not going to get you too far.

Bob Maley: Right and I learned that lesson a long time ago when I was a cop that home security, basic home security is locking your front door. It's like why should we lock our door? Nobody's ever bothered us here and it's because nothing's ever happened and when something bad happens in the neighborhood, well then it hits home and it wakes people up. The problem we have here is our neighborhood, it's the entire commonwealth and so we have been fairly good at preventing serious problems. We've had them in the past obviously like there's been publically announced back in 2007 data breaches. But we've put in some significant programs in place that have reduced those to almost nonexistent and that's great but that doesn't mean that something's going to happen tomorrow. I can't say that. So I can't say I need more money because it may happen tomorrow.

Dennis Fisher: Right.

Bob Maley: So what we've done is we've actually shown through one of our programs that we have we are very proactive in looking for problems that we might have before someone else finds them and I imagine the private sector may have similar challenges to what we have is that when IT grew up here in the commonwealth it wasn't centralized. Every person that had a need that knew how to program in BASIC or when we moved on to Visual Basic or all the different types of things, Microsoft Access, everybody started doing their own programs. Oh you know I do web development, here I can stand up an application and this will really help us do that and I think a lot of those types of things, the legacy things that are out there are serious holes.

Dennis Fisher: Yeah.

Bob Maley: So we've done very proactive and we still do this on a regular basis. We go out randomly. We do pin testing. We try to hack our own systems and in 2008 we found holes that would have exposed 400,000 records of confidential information and through our forensic follow-up and investigation we found we were the first ones to find those, that we had to beat the bad guys to our own problems and close the door and the cost avoidance of data breach notifications was significant. Using some old numbers at \$90 a record, we showed that our programs are returning a result of \$38 million in cost avoidance to the commonwealth.

Dennis Fisher: Not to mention the bad publicity avoidance which is always nice.

Bob Maley: Yes. Yeah, we have to stay out of the press.

Dennis Fisher: Yes, that should be a goal every year I would imagine and you found that through pin testing you said.?

Bob Maley: Mhm.

Dennis Fisher: It must have been a good feeling to once you went back and tracked through it to be able to figure out hey okay we were the first ones to find it. We can't find any evidence that anybody else has gone through this vulnerability aside from us.

Bob Maley: Yeah, extremely.

Dennis Fisher: Okay.

Bob Maley: One of the good things though is since we are the government we can keep our logs forever and the follow-up forensic investigation may be time consuming but to be able to go back to the first date that an application was deployed and investigate all the logs, all the access, all the things we looked at to determine whether we were the first ones or not is very good to be able to demonstrate. We did find this. We were the first ones in.

Dennis Fisher: Nice. So it sounds to me that you fairly early on were able to win some friends high up in the organization there to get on the side of your security programs.

Bob Maley: Yeah, that's been since day one. I understood when I had come into the role how the environment works and without that senior management buy in to what we're doing it really was just

the temporary type process. If I wanted to develop a program that was successful, that was high yield recognized, that I could go into those environments and speak to the senior level people, that they took what we were talking about seriously, and that was from day one that I had to do that and have been very good at doing it.

Dennis Fisher: Yeah, I feel like that's another mistake that a lot of guys in other organizations make is that it may be through no fault of their own because they're busy doing their jobs a lot of the time especially if it's a small organization and they're doing operational things as well as the management and planning and all of that sort of thing. They don't necessarily have the time to sit in on big meetings and kind of do a little politicking to win friends for their department and get support for the programs that they might need down the road.

Bob Maley: It's the changing role. I've seen NASCIO I think did a paper on it. I've seen it in many magazines, anything that's based around CISO or CSO, the changing role of the CISO and it is significant because a lot of folks came to that position through their technical competency and their technical expertise and while that's good, being able to connect to your business people and understanding the business of your company or in our case the government. For instance our state police, they have a very different business model than the department of public welfare and they have different needs.

Dennis Fisher: Sure.

Bob Maley: When you understand that instead of trying to come down as well like I'm in charge, I'm at the top, and you guys all do what I say, when you go in and you understand what their needs are before you do any of that and you incorporate their business needs into your programs, you do that a couple times and it gets really easy.

Dennis Fisher: And it also I would guess pays dividends even if they're not immediate. It's got to pay dividends down the road when you've got a pet project or something that you think is important and maybe it's not getting the support it needs. You can sort of go to these guys and say listen this is really important. It may not look like it now but trust me.

Bob Maley: Absolutely.

Dennis Fisher: Yeah.

Bob Maley: Credibility, it builds your credibility.

Dennis Fisher: Yeah. How much user education have you had to do in your time there? Is that a big initiative inside the commonwealth?

Bob Maley: Well it's huge in my book. It's difficult to do given the size of our environment and the disparity of where employees work. We were able to get a policy that requires very commonwealth employee and contractor to undergo annual security awareness training. We do other types of events. We're pretty involved with the Multi-State ISAC so every October we do our annual cyber security awareness month. In the past we attend conferences with tables so we can get our message out not just to commonwealth employs but local government as well throughout the state and it is key because the change in the threat landscape that we've been seeing, not just recently (I know a lot of magazines are talking about lot now) but we've seen it for about a year and a half, almost two years now is that the vendors out there with technical controls are very, very good. There are a lot of very good things that we can put in place and they work. But the bad guys, well, when they're stopped one way they're always, well let's find out what's our next avenue, how do we make a compromise happen and if we've really got ourselves protected, we have that hard crunchy exterior, we have all the multi-layers of defense so if they get through one hole we catch them. We have all those things and it works really great. But the one layer that is most vulnerable and is very difficult to secure, it's the human layer.

Dennis Fisher: Sure.

Bob Maley: And we have some here that our vulnerability, attacks against that layer have increased significantly and so we're making as much effort as we can for the security education, the security awareness. We do updates now every time I get a chance to go and do a presentation someplace or any group of stakeholders. I'll do that to try to educate the folks about staying safe on the internet and the basics and we can't say this enough, not to click on a link that you get in an email. I know for security pros it sounds so, well, duh, but most folks out there aren't security pros and they don't understand and it's that prurient interest that's, "Oh, I bet this will be cool," and then usually they always have that oh no factor after they've clicked and it's too late and the damage is done.

Dennis Fisher: Right, yes.

Bob Maley: So that security awareness, the education of our end users is always going to be a high priority and were going to always look at whatever we need to do to make it better, to reach more people and reach them more often.

Dennis Fisher: Did you encounter any resistance from the end-users when you started the user education program?

Bob Maley: Yes.

Dennis Fisher: And how did you get by that?

Bob Maley: There was an executive order requiring employees as part of their employee training.

Dennis Fisher: That helps, yes.

Bob Maley: That helps, yes, it's a big stick.

Dennis Fisher: What about high up? Did the managers or the people running these disparate agencies say listen we're busy collecting tolls or doing whatever it is. We don't really have a lot of time for our guys to go through this?

Bob Maley: I'm sure there were those types of comments made but we've been pretty successful with it. I think people are starting to understand that the assets that we do have, although we don't have stock value, we don't have those types of things, we have significant assets and confidential information about citizens and I think senior management recognizes that and takes it seriously and of course obviously it's not 100%. There's always somebody who's not going to be on board but we have really done well. We've had people buy into the understanding that we are the keepers of a very significant asset and we need to treat it as such. So it's gone over pretty easy.

Dennis Fisher: Okay, that's good. You mentioned earlier on in the podcast that you guys did have that data breach a couple years ago and you've put in some things to ensure that doesn't happen again. What kinds of things did you do? Did you go down the road of encryption and those sorts of things?

Bob Maley: Yes, every mobile system in the commonwealth is required to be a ____ disk encryption. We've enterprise-wide intrusion prevention and intrusion detection on every host. We have a SIM in place that we're collecting about a billion events a month that

get correlated, allowing us to look at trends, look at the areas that may be problematic. Already we've used that to identify some SQL injection attacks that were underway that reduced a potential breach of 40,000 records down to 2, so those types of things. All the different programs that are in place and, again, we're continuing. We're moving forward as well. We're currently implementing a third party email encryption so that all commonwealth employees that need to exchange information outside of the commonwealth they can be secure and be encrypted very easily. It allows us to put in the compliance tools as well that doesn't count on an employee thinking about it. It understands and it sees this should be encrypted, so that type of a tool. We don't have everything in place but those things are coming out now as well. So we've just tried to stay current with where our threats are and it's been successful. We've reduced those information problems and we've been proactive in discovering those that may hit us down the road as well.

Dennis Fisher: Yeah, yeah well it's good to see that people are certainly utilizing the tools that are out there, especially on the mobile devices which, you know, I feel have gotten a little overlooked a little bit. With the amount of data that they can carry now and the fact that everybody is sending corporate email with attachments and that sort of thing from them and have been for a couple of years now, that's a major sort of weak spot in a lot of networks I feel like.

Bob Maley: Yeah because the rest, it's pretty secure. Those areas like you were talking about, previously nobody even thought about them but now they are the avenues that the bad guys are going to try to figure a way to exploit.

Dennis Fisher: Yeah, alright well listen, Bob, I appreciate your time. I'm going to let you get back and help protect the citizens and I really appreciate it and it was good talking to you again. Hopefully we can do it again sometime.

Bob Maley: It was good talking to you as well.

Dennis Fisher: Alright, take care Bob.

Bob Maley: You bet. Have a great day.

Dennis Fisher: Thanks.

Anatomy of the RBS WorldPay Hack

The four men whom a federal grand jury indicted this week for their alleged roles in a scam that stole millions of dollars from RBS WorldPay were no fools. The small crew of hackers had a distinct division of labor, operated with skill and efficiency and left one of the world's larger banks holding the bag.

Viktor Pleshchuk, Sergei Tsurikov, Oleg Covelin and a fourth man, identified only as "Hacker 3," pooled their talents, and with the help of a worldwide network of "cashers" in more than 280 cities, they were able to walk away with \$9 million of RBS WorldPay's money. The attack, detailed in a federal indictment announced Tuesday by the Department of Justice, illustrates clearly the level of organization and sophistication involved in ATM and payment-card fraud, as well as the difficulty banks face in guarding against these schemes.

The scam began simply and came together quickly. In early November 2008, prosecutors allege that Covelin discovered a vulnerability in the network of RBS WorldPay, a subsidiary of the Royal bank of Scotland that handles payroll and other payment-processing transactions for companies around the world. Covelin took his find to Tsurikov, who in turn brought in Pleshchuk, the man who had the technical skills to exploit the vulnerability. Tsurikov allegedly acted as a kind of social director throughout the scheme, bringing together various people, matching up a need with a skill set.

On Nov. 5, Covelin allegedly gave Pleshchuk a username and password for a server on the RBS network in Georgia. Once inside the RBS WorldPay network, the hackers, led by Pleshchuk, allegedly gained access to a database containing the account numbers and PINs of payroll debit cards that the company's customers give to their employees in lieu of live paychecks or direct deposits. The cards allow employees to withdraw funds directly from ATMs, up

to a pre-set limit, or buy merchandise from approved vendors.

See related story: [U.S. Takes Down \\$9 million RBS WorldPay Hacking Ring](#)

The indictment does not spell out the exact structure of the database that the hackers allegedly compromised and makes no mention of encryption of the data set. But, the attackers were able to get both the debit card account numbers and the PINs associated with those accounts. It's unclear whether the account numbers and PINs were stored together.

After getting that data, Pleshchuk, Tsurikov and Hacker 3 allegedly went in and jacked up the amount of money available on the debit cards and raised the withdrawal limits on the cards, as well. The trio then sent 44 prepaid payroll card numbers and PINs to a pre-arranged network of "cashers." Typically, someone in these networks takes the numbers and PINs and creates a fake card programmed with the data.

Then, just three days after the crew's first foray into the bank's network, on Nov. 8, cashers in 280 cities around the world began hitting ATM machines, withdrawing predetermined amounts at each one and then moving on to another terminal. Within 12 hours, the crew had stolen more than \$9 million from RBS WorldPay, a massive one-day loss even for a company the size of RBS.

Meanwhile, Pleshchuk and Tsurikov allegedly went back into RBS WorldPay's network to monitor the activity while the cashers were making their rounds, ensuring that the mules did their jobs. The hackers were letting the cashers keep a sizable portion of their withdrawals--between 30 and 50 percent--so they wanted to know exactly how much money would be coming their way.

Spotlight Series

After the attack was over, Pleshchuk and Tsurikov allegedly went into the RBS WorldPay database logs and began deleting any information that would point to their scheme, according to the indictment. But the crew apparently didn't do a very good job of covering its tracks.

After the attack was over, Pleshchuk and Tsurikov allegedly went into the RBS WorldPay database logs and began deleting any information that would point to their scheme, according to the indictment. But the crew apparently didn't do a very good job of covering its tracks.

Security officials at RBS WorldPay noticed the fraudulent transactions quickly and reported them to law enforcement. And now, Pleshchuk, Tsurikov, Colevin and Hacker 3, along with four alleged co-conspirators, Igor Grudijev, Ronald Tsoi, Evelin Tsoi, Mihhail Jevgenov, are facing federal charges and several years in prison for their trouble.

About Threatpost

Threatpost, Kaspersky Lab's Security News Service, is dedicated to helping IT security professionals succeed by delivering the most important and immediate security news and analysis available.

Threatpost offers a fresh approach to providing up-to-the-minute news and information for IT security and networking professionals. Threatpost editors cover today's most relevant security news and the most pressing security issues of the day. They break important original stories, offer expert commentary on high-priority news aggregated from other sources, and engage with readers to discuss how and why these events matter.

Threatpost's global editorial activities are led by industry-respected security journalists Ryan Naraine and Dennis Fisher. They bring over twenty years of experience to their mission of delivering insight into the issues that affect the lives of security professionals every day.

Threatpost has expanded with Latin American editions in both Spanish ([link](#)) and Portuguese ([link](#)). These editions are led by local, veteran editorial teams dedicated to covering security news and analysis vital to the region.

Make Threatpost your first stop for security news and analysis.

www.threatpost.com