The Reality of a Cyber Incident and Why Cyber Insurance Isn't Enough

2026 National Conference

ROB TARLETON: How are we doing, everybody? It's a smaller group, so we're going to have plenty of time for Q&A. You can stop me and ask questions or whatever. Feel free. I know where you all are. I have the scars to prove it. Myself and my business partner, Terry Ann, who's down here in the front. Between the two of us, we have over 30 years of performing arts and cultural nonprofit symphony experience. I spent 15 years as Lincoln Center's Chief Technology Officer through the beginning of COVID. Terry Ann spent about the same amount of time at the New York Philharmonic and NJPAC before there.

So we've lived your world. We have the scars, the same scars as you all have. So please feel free, stop me, ask questions. There'll be plenty of time afterwards as well, I think. So I want to start with a couple of questions. How many people here know an organization or know somebody that's been hit with some sort of threat actor, cyber event, ransomware, account takeover in there, right? Yes, a lot of folks in here. How many folks' organizations—and feel free not to tell on yourselves if you don't want to—have been hit personally in their organizations with ransomware or with account takeovers, with whatever? Yes, a lot of organizations have. I know I have. How many people in here have sat there and thought through what they would do if their organizations got hit with a ransomware or other type of threat, cyber threat event? Yes, I have too. I went through it in my head. I tried to figure out what I would do in all these scenarios. We'll get into that one in a bit.

[00:02:04]

Sadly, I never thought that we'd be this involved in cyber. That was not Double Eagle's original focus. It is not our major focus now, thankfully, but Double Eagle has personally run, I've personally run over three dozen ransomware events in this cultural non-profit vertical in the past four years. And it's a shame. And thankfully, most of them were on the smaller side. There were a couple that absolutely were not. So I want a level set first. If a hacker wants to get in, they will. These folks can hack into the US Department of Defense and NORAD. If they want to hack into our environments, they will. It's just that simple.

Our job as technology and cybersecurity professionals is to make it hard enough that they'll get frustrated and go elsewhere because they don't want to work hard for this. They want it to be easy. They want to get in. They want to get something that they can ransom for you. They want to get out. If we frustrate them long enough, they'll go somewhere else. That's the focus because, quite frankly, time is on their side. It's just that simple. So my own version, I believe it's probably going to be relatively close to your own, when I thought how

things would go in a cyber event in my organization was, "I have cyber insurance. I'm good." I have an event. I call my agent. I tell them that I've had an incident. They assign a law firm to me. They assign a firm that's going to help me fix all these things.

[00:04:02]

I have backups that are air-gapped, that are off-site. I restored the backups. We're good to go. How many people in here think that's relatively close to what you thought originally? I know I did. Originally, when I was thinking in a vacuum. Yeah, no. It goes nothing like that. As a matter of fact, the reality bears zero resemblance to that. The fact of the matter is, that wonderful person that you've been talking to from your cyber insurance carrier is going to turn into the auto accident version of your auto insurance carrier. Because the minute you call and tell them that you've had an incident, they're now interested in finding out how much it was your fault, so that they can mitigate to the largest extent possible the amount that they are going to pay you and pay out as it relates to this event. That's what's going to happen. And they are assigning you a forensics firm. I use that term very specifically. That firm is on a statement of work from the cyber insurance carrier to find out who, what, when, and how. And to handle direct communication with the threat actor if that's necessary. And everything they find out is going to go back to the cyber insurance carrier to try to identify how much of this is your fault, so they can mitigate the amount they're going to pay. It is your responsibility, as the organization in this event, to stop the threat.

[00:06:01]

They'll tell you how they're getting in. It's up to you to physically close the door. They're not going to help you. It's up to you to clean all the devices that have been breached. They might give you a tool to use, but they're not going to help you do it. You need to do that. And they're certainly not going to help you rebuild. That's on you. Most organizations do not have the human resources available to do that themselves. You need a list of experts that you can call that are on your side because you're going to need to do this yourselves. Now, this forensics firm, they will do this work for you under a separate statement of work to you that you will pay for, that the cyber insurance company will probably cover. But see statement one, everything they find out will go directly to the cyber insurance firm, so they can figure out how much they're not going to pay on the policy.

So you need somebody to help you with this work that's on your side. That's going to help you recover this. That's why we say you should have your own remediation firm. Your cyber insurance carrier will pay that. They will not pay for duplication of services. So if your remediation firm is doing forensics work, they maybe use that word "forensics." The cyber insurance company will not pay that third party because they assigned a firm to do that already. So they're not going to pay twice. But if this is the firm that's yours that's going to

help you clean it up and restore remediation, they will pay that. It's literally a game of semantics.

[00:08:01]

It's a game of words with them, whether they're going to cover it or not. So you need that firm. You need a firm on site that's going to be able to be those additional resources you need. Experts in network and servers, physical hands because in a lot of instances you have a lot of servers and a lot of computers that all need to be completely wiped and reset up. That takes time, and that takes people. You need to know that you need that. So you need that list.

What a lot of folks don't realize is that thought of having a backup—"I have my backups, they're air-gapped. I get them, I download them, I restore them. I'm good." Well, yes, in theory. In practice, every device that's compromised is quarantined by the forensics firm. You cannot touch it until it's released, which means where are you going to restore your backups? It's been hit. It's quarantined. If you start to do your clean and restore before the forensics firm releases the hardware to you, the cyber insurance company won't pay. And in some instances, in most instances it's a couple of weeks. In some instances on the far side of this, I've seen it be six to seven weeks before they'll release that hardware. So you have backups, but you need to have planned where you're going to restore them to. Because unless you have hardware sitting on the shelf someplace—and almost nobody has that anymore—where are you going to restore the backups to? You could have an Azure or AWS Amazon Web Services environment that you could restore to, but that has to be planned in advance. That's where your business continuity has you restoring. This is all stuff that you don't realize.

[00:10:04]

Now, how do you have that not happen? How do you become, I put this in quotes, air quotes, "ready?" What does that mean? That means that you are prepared to the greatest extent possible so that your downtime and/or business continuity strategy will be as short as possible. Number one, if you don't spend another nickel on cyber, you need to do the first two things. I refer to them as 1A and 1B—annual penetrations testing and vulnerability scanning. Absolute must every year. Too many of the incidents I've been personally involved in would have been solved by a penetration test that identified gaps in the firewall or other open avenues to the Internet that the institution didn't know about. Then in large cases was opened many, many years ago before the current IT team was even on site, and they don't even know they exist. A penetration test would have identified that, and you could have closed it. It's a simple, relatively cost-effective fix as far as increasing your protection.

The next one, it's confusing. It's alphabet soup in the industry. Is it EDR? Is it MDR? Is it MXDR? I refer to it as three levels, right? Your computers and servers, your endpoints—desktop computers, servers, etc. Your network is your next layer—physical traffic, firewalls, domain controllers, etc., and then your cloud entities because everybody's got cloud-related entities that need monitoring today, whether you're a Google shop or a Microsoft shop, whether you've got resources up in Microsoft Azure or AWS or the Google Cloud.

[00:12:05]

All three layers need to be protected. And most organizations that are our colleagues do not have the staff to manage that monitoring themselves. They don't have the physical resources. You need a security operation center that's looking at this, all of these layers of telemetry, 24-7, 365, that you've given the permission to remediate stuff on the fly. Because threat actors never kick off anything that they want to do at noon on a Wednesday. They don't. It's 3 a.m. on Saturday morning on a holiday weekend when they're hoping that they're going to have three days' run time before anybody sees the alert. So you need somebody looking at it at that time that can remediate it then. And there are a lot of firms out there that do it well. We do comparative analyses between the top three or four for our sector here all the time. Gradient Cyber seems to win most of the time.

The next thing is you need robust access control policies. And I'm not talking about a physically written document. I'm talking about the policies up in Microsoft Entra or in your Google access control area that controls who can access what, where, when, whether that is country blocking, whether it is policies like impossible travel, whether it is policies like risky user, risky sign-in. Multi-factor authentication everywhere on everything. If you're not being challenged for a secondary form of authentication on any application, whether we're talking finance, payroll, development, obviously email, all of it.

[00:14:12]

If you're not being challenged, ask your IT people why. Because you should be. You should be multi-factor on everything. Country blocking is huge. Do you really need somebody trying to log into your VPN or your email from Russia or China? Do you need them trying to access finance or payroll from Russia or China or North Korea? Probably not. Emails are a different story. A lot of folks have orchestras that travel. So to that extent, your country blocking policies for your email may be more lax than for your business systems. You can and should have multiple country blocking policies at different strengths, based on the applications that are connected to them. This is the start. This is the physical network side of how you don't end up with a massive ransomware incident.

As far as the cloud goes, there is a direct correlation between the amount of onsite on-prem applications you have and the length of time to recover from any incident. The fewer the applications you have locally, the shorter the time to recover. And you'll see a scenario that I'll walk everybody through later on of exactly how quick that can be, even when you get hit with ransomware. You need to talk to the entire organization, develop a roadmap and a strategy for migrating any applications you have locally to the cloud, whether those are traditional file shares that should go to Google Drive or SharePoint, or whether it's an application, whether it's finance or payroll or your ticketing environment.

[00:16:15]

And I have a scenario where you see how important those migrations become. Again, I mentioned move local files to the cloud. Google Drive, SharePoint, right? I mentioned it earlier: Backups in the cloud, air-gapped, encrypted because you will have had need for them. Create a scenario where you're restoring those backups. Do not rely on local hardware. Have an Azure or Amazon AWS instance set up. And you can have your entity shut down so it's not costing you money, but have tested that. Know where you're going to restore those backups.

Cloud-based device management. All of the devices, laptops, cell phones, they all should be managed by, if you're a Microsoft shop, Intune. If you are a Google shop and you're mostly Mac, use Jamf, but it all should be managed at that level so you can control the profile on these, so you can control the patching, so you can control what these folks can access or not, so you know the safety and security of the devices that are connecting to your applications and your network. Cybersecurity is an organization-wide issue. It's not just IT. You should have an annual cybersecurity assessment by a third party. Make sure all the I's are dotted, T's are crossed.

[00:18:02]

You should be having cybersecurity discussions in your executive leadership meetings. If you're not hearing those discussions, bring them up. Be the person that brings up the topic. You should be having cyber preparedness and status discussions at your board level. If you're not, have those discussions. Be the person that starts those discussions. Organizations that keep cybersecurity top of mind are least likely to get hit because they're talking about it, which means they're executing on it.

Staff education is the biggest thing you can do to help yourselves, whether you're going to use KnowBe4, or whether you're going to use any other of these education tools and testing tools. The past year, I have seen very few ransomware attacks. I've seen six to seven a month of account takeover, which was all started by really, really good spear phishing

attempts, where people were fooled into clicking something or giving their username and passwords to somewhere.

Account takeover. I see five, six of those a month. I have three investigations that other organizations in our vertical here have asked me to ask them how it happened, that we're doing right now. Education. So, assuming you get hit, what do you do next? You have to have an incident response plan. Most everybody in here has a credit card compliance PCI regulation that they're responsible for because you all sell tickets.

[00:20:06]

Maybe it's not yours. Maybe it's the venue that you perform in, and it's their ticketing system. So then they would have it. Having an incident response plan is required under the PCI data security standard in order to be PCI compliant to your banks and your financial entities. So you have to have that, and it should be exercised. You need to run mock cyber security incidents with the entire team that's involved in—that would be involved in this. Everybody's got to know what they need to do because without it, I mean, these events are hairy. Everybody's hair is on fire. Emotions are up. If somebody doesn't know their roles here, it's going to be far worse than it needs to be anyway.

What happens when you're prepared? This organization got lucky. We were working with them.

We rolled out SentinelOne with network protection, with a SOC on there, and as you can see here, we rolled that out. And seven minutes after we pushed it live, the London SOC, because it was 8 o'clock at night, so the security operations centers follow the sun. The SOC in London got a hit that there was a ransomware signature waiting to execute and quarantined the development staff member's computer from London and kept that from executing.

[00:22:04]

The money they spent on this ROIed in seven minutes, because had that executed, it would have cost them millions of dollars. Any questions before I go into the case studies? Anybody have anything running through their head? Please.

QUESTION: What is a ransomware signature?

TARLETON: So great question. Somehow a threat actor gets access to your network. Maybe it's a staff member that clicked on something that they shouldn't have. They had access to their computer. Once they have access to your network, they put a program in a couple places on your network that they can execute with a single command. While they're doing

that, they're perusing your network to see what they can find. So they find backups, they're going to encrypt them immediately if they can. Where is the data? Oh, there's a file share here. They're going to take all of that, and they're going to exfiltrate that. They're going to send it off to wherever they are, hoping that there's social security numbers, credit card numbers, or passport numbers, or anything that they can sell in there. They're going to hope that there is confidential information there. And they're going to wait. And they're going to look around.

It's amazing. The ransomware events that we've had, the ransom that the threat actors have asked is the exact amount that the cyber insurance is for. Why do you think that is? It's because they found the policy on somebody's file share someplace, and they know exactly what the cyber insurance company will pay. They've already got it. They know exactly what it is.

[00:24:01]

And then when they're ready, they press the go button. And then this thing starts to encrypt everything it can put its hands on. It's just waiting. So all of those procedures and things that I just talked about, they are an attempt to what they refer to as "kill the attack chain, right? Break the attack chain. The first thing that all of these programs do is they call home. I'm awake. What would you like me to do? They're always calling home to somewhere that you would have blocked from a country blocking perspective on your firewall. If they can't call home, they can't execute. They will not execute unless they receive the go and what to do.

So if they're calling home to Russia, for instance, and you have Russia blocked on your firewall, it won't execute, which is why all of that stuff is important. Right? Should you ever have a program inside your network, a computer in your network, calling out to Russia or China or South America? Probably not. Selling tickets in those areas is cool, but that's not what we're talking about. We're talking about direct access to your network. That's a great question.

And by the way, folks, I've tried to make this as non-technical as possible, although it's a technical discussion. So please, feel free, ask. We actually have a mic for questions. Go on. So what it looks like to be what we'd consider an organization that is high-maturity.

[00:26:05]

You will have talked to your cyber insurance company. You'll know what the coverage is. You will have found out who is on their list for remediation. I know a lot of these folks on a first name basis by now. You will have your own organization on a remediation retainer. Double Eagle does offer one, zero dollars. All the T's and C's will be taken care of ahead of time so

that if something goes bump in the night, we're your phone call. First or second, either to us first and the cyber insurance company second, or vice versa. But have one. That level of the three layers we talked about, the most important dollar that you can spend. Proper software on your computers and servers, proper detection and monitoring software on your network, proper monitoring software for your cloud properties. All of them, all tied to that security operation center that's a resource for your team, 24-7, 365.

Take the time. This organization took the time, created a strategy, migrated all of their applications to the cloud. They went through a SharePoint and OneDrive migration. They migrated their finance application to the cloud. They migrated a couple other applications to the cloud.

[00:28:03]

They installed Intune and put that on all of their computers, laptops and their company cell phones. They got rid of as much of their on-prem server footprint as possible. To date, there has not been a breach that started off in an organization and migrated to any of your cloud properties so far, because those are physically disconnected from your network. You can't get from point A to point B. I have a caveat for that. It just came up a few weeks ago, having nothing to do with the ransomware and everything to do with account takeover. But I'll get to that later. Create that incident response plan. Have it published throughout the organization and run a mock exercise on a regular basis so the organizations know what to do if you are unfortunately the victim of some sort of cyber incident. So everybody knows their piece.

Those incident response plans—they should have in them templates for email that communication would use. They should have in there templates for communication that marketing would use on your social media or to your ticket members. They should have mock communications, templates in there that communications would use if you have to talk to the media. So all of that stuff, it's not just an IT thing. It's having that stuff ready, so you're not trying to write something from scratch with your hair on fire.

[00:30:00]

Medium cybersecurity. This is the incident that I was talking about that has a couple of things in it. At 4:00 a.m. on a Wednesday, this firm did what they needed to do. We had them back up with zero business system interruption in 72 hours. Why? They replaced their antiquated firewalls with new ones that had the ability to have country blocking and IP and domain threat actor subscriptions on them. They migrated all their critical applications to the cloud. And as a matter of fact, this happened on a Wednesday. The previous Friday, they moved their Tessitura instance from on-prem to Tessitura hosted services. Lucky that it

happened literally days before the event. They had multi-factor authentication on everything. They installed the three layers of security that we talked about. They had SentinelOne on the endpoint. They had something monitoring the network. They had their cloud properties monitored properly. What happened?

Only three servers were accessed. The SOC picked it up and locked it down and quarantined those three servers and blacklisted the program that was trying to encrypt things throughout the rest of the network. And those three servers had nothing to do with anything production. Because the only production—the only business systems they had left on-site was the building management and physical security. They moved everything else to the cloud. And the Tessitura environment had moved out the previous Friday, so it wasn't even there anymore. Pure luck.

[00:32:03]

Nothing was encrypted. Nothing was stolen. They didn't have a chance. The SOC locked it down. At four o'clock in the morning, had they not had that security operation center, this would have kept going until somebody from this organization saw it, which would have been hours later. What did we have to do? We figured out where they came from and closed it, obviously. We scanned the entire environment. Out of an abundance of caution, we changed all the passwords. We had everybody change their passwords on everything, just because. We were able to restore the backups because they had other hardware, because remember, the affected servers were very small. So we had another environment that we could restore the backups on. All the passwords were changed. What was learned?

No service account should ever have VPN access. What does that mean? For those that aren't part of IT, there are service accounts in everybody's network, and the applications and services that you use every day use these service accounts, use names and passwords to execute on your network to run. Somebody years before this set of IT people at this organization, because it was just easier, they could maintain the application from home if they gave the service account VPN access. Well, service accounts typically don't get their passwords changed. And service accounts don't get multi-factor authentication because they shouldn't ever need it because they should never have public access at all.

[00:34:05]

So somebody years earlier had done this. The organization didn't even know this existed. So no service account should ever have VPN access. All passwords need to be changed regularly, and all VPN accounts have to have MFA. They have to be multi-factor authenticated.

The final scenario, case study. When the executive director of an organization calls you at 6:31 a.m. on a Thursday morning while you're having coffee, watching the news. You don't know what it is, but you know damn well, it's not good. That's real. That happened. This event actually started at 3:20 a.m., and the time to resolution was 3-and-a-half months. And all of their critical systems were down for over three weeks. That includes payroll. That includes fundraising. That includes all ticket sales. Everything. Why?

They had stopped, like a lot of organizations, they had stopped upgrading their technology over COVID. And it was antiquated. And it should have been replaced. They were using standard antivirus, McAfee, stuff like that, not the zero-day quality we were talking about, SentinelOne and CrowdStrike, and that sort of thing, right? They hadn't done a penetration test in many, many years.

[00:36:00]

And they didn't have any monitoring in place to tell them when things were going wrong, when things were failing. So as things failed, if it wasn't super public, like the database server for the website, for the ticketing system, went down—unless it was massively critical like that, they didn't know stuff was falling offline. They had no visibility into it. What was compromised? Everything. And I mean everything. Every server, every desktop, everything that was connected. Everything. They got over three terabytes of data from their file server environment on there. They only ever recovered one. There are two terabytes that are gone forever. What did we have to do?

Well, again, you have to close how they got in. Stopping this replication was hard. It was flying everywhere. We had to scan the entire environment machine by machine to figure out whether it was involved. We had to rebuild every single laptop, every single desktop, every single server from the ground up. Their backup environment was not air-gapped and encrypted. They encrypted the entire backup environment. We found a copy of their ticketing system database on a server that had been turned off a short time earlier that was 14 days old. So they had to try to recreate 14 days of transactions once we found that.

[00:38:08]

Thankfully, they had a university across the street that they were very friendly with, that it just decommissioned a bunch of servers. They called the IT people from the university, picked up the servers that they just pulled out of the racks and literally walked them across the street and handed them to us to plug into the wall so we had some hardware to start to restore things to. Because remember, you can't touch the hardware once it's encrypted until the forensics firm releases it, which didn't happen for six weeks. Obviously, you're changing

passwords. They had to systematically try to rebuild 14 days of transactions on the web, and they had an on-sale in the middle of that, by the way. What was learned?

Tech debt has consequences. Not paying attention to the infrastructure that you have and keeping it updated and making sure your IT people are keeping it updated. Again, this whole thing could have been solved, could have been prevented with a penetration scan. Somebody had left the port open on the firewall when they migrated from an on-prem email server to Microsoft 365, and that port of the firewall was never closed. A penetration scan would have picked that up. They would have closed it. This entire event doesn't happen then. Where do you go for help? What should we be looking at? CISA, Cybersecurity and Infrastructure Security Agency.

[00:40:04]

They are the cyber people attached to the Department of Homeland Security. If your IT folks have not signed up for CISA alerts, they come on a regular basis. Whenever there's a vulnerability, CISA will send out an email blast. Maybe you don't have Palo Alto firewalls, and you don't care about the one that just came out yesterday. Maybe you have Palo Alto firewalls, and you do. That's why you sign up for those alerts. CISA has all kinds of self-help manuals and forms that you can fill out. Self-assessments that are available on their website, that mock cyber incident that we talked about. If you contact them with enough time in advance, they will come on site and help you run that. Right now they won't because they're not funded, so they're not allowed to do any of that. We actually run those red team exercises for organizations if you want.

Here's the URL. They have a lot of information out there. They're great people. You should know your local CISA rep. Your IT people should.

It's been wonderful spending this hour plus with you all. Thank you very much for your time.

[00:41:37]