Below we have provided the scripts that go along with each Virtual News Network (VNN) inject video that is included in the TTX PowerPoint. Additionally, on-screen text and imaging is described throughout in ***bold, italicized text***.

Script 1 (Length 3-5 minutes): Background information and exposition that sets the scene for the story playing out over this and the next two script installments is delivered via a VNN news piece about a threat delivered by a global hacktivist network who call themselves "The Void."

On Screen: VNN logo animation
For this and all scripts that follow, the "EXERCISE EXERCISE EXERCISE" watermark will be applied graphically, throughout.

On Screen [News Ticker]: BREAKING NEWS

Jeanne Meserve:
Welcome back to Nightly News. I'm Jeanne Meserve, live from VNN headquarters in Washington, DC.

On Screen [News Ticker]: Zero Day Attack
Global Cyber Security Scare

Jeanne Meserve:
Our lead story in business today is a cyber security scare of potentially global proportions. A network of hacktivists known as The Void today threatened to unleash, and I'm quoting here, "a global day of extreme action against U.S. interests and organizations, both private and government-related."

If you need a digital terminology refresher, hacktivism involves the nonviolent use of legal and/or illegal digital tools in pursuit of political ends. In the past, The Void has come out against the Global Trade Summit and other trade and finance related institutions, as well as independent companies.

On Screen [News Ticker]: Zero Day Attack
The Void: Against the Global Trade Summit, Finance Institutions, Independent Companies

A section of the message text from The Void speaks of a "Zero day attack."

On Screen [News Ticker]: Zero Day Attack
Attack Which Will Exploit Computer Vulnerabilities Unknown to Their Users

That's an attack which exploits computer system vulnerabilities unknown to others, even the software developer. And tonight there are indications that The Void plans to—or has already—gained access to the systems they're going to exploit.

On Screen [News Ticker]: Zero Day Attack
Indications Suggest The Void May Have Already Gained Access to Systems

The Void's message was sent to several reputable online news sources including Global Net News and buzzcode.org, and several cyber security experts are confirming that the message did indeed come from The Void.

How do they know that? Well, they conducted an independent analysis of the source code and also examined how the message's Internet Service Provider was concealed. They found digital traits similar to those found in previous threats from The Void.

On Screen [News Ticker]: Zero Day Attack
Previous Attacks: The New York Trade Index Which Disabled Trading for a Whole Day

You will remember that one of those threats was sent to the New York Trade Index last year and The Void subsequently acted on it crippling the index for a full day.

And that is why today's threat is being viewed as very serious.

Jeanne Meserve:
In a VNN exclusive, we're being joined by a former hacktivist who is now on the other side of the fence working with companies and organizations to improve their cyber security, by trying to hack into them, himself. His real name and identity are being concealed to protect his own security. We're going to call him Jake.

On Screen: Hacker is concealed by silhouette and voice modulation. His lower-third identifying info reads: "Jake," Hacker Turned Security Expert

Jeanne Meserve:
Hi Jake, and thanks for joining us tonight.

Jake:
Thanks for having me on.

Jeanne Meserve:
What can you tell us from a hacker's perspective about today's threat?

On Screen [News Ticker]: Zero Day Attack
The Void has Always Followed Through on Attacks 100% of the Time

Jake:
Well, like you said, this is serious. The Void has always delivered on their threats in the past, one hundred percent, and that's not good news for whoever they have in their sights.

Jeanne Meserve:
So after looking at the message from your perspective, is there any indication of exactly who the target might be?

On Screen [News Ticker]: Zero Day Attack
Anyone Could be a Target in This Cyber Threat

Jake:
Really, it could be anybody. I mean, they've gone after small businesses for their export or even labor policies, gone after big businesses for global and trade stuff, and of course Wall Street last year. I still haven't figured out some of the details that went into that one, and I've been looking at it for months.

In general, small to medium sized businesses do tend to be easier targets, though, since they usually don't have the security resources that big companies do.

Jeanne Meserve:
So what exactly would you say to anyone trying to protect their company or their organization from an attack like this?

Jake:
Apart from hiring me – I'm just kidding! – I'd say that everyone – from small businesses to huge companies – needs to know the rules.

People are working from everywhere now, using a laptop for work and for personal things, so they need to know how to keep safe.

The bad stuff I uncover for companies usually deals with employees who don't know what's cool and what's not cool, like randomly downloading software, plugging into unsafe networks, losing things like external hard drives or thumb-drives that aren't protected, that's how companies expose themselves to hackers, thieves, and scammers.

Jeanne Meserve:
Thanks, Jake, for your insight.

Jake:
Any time.

On Screen [News Ticker]: Zero Day Attack
Know the Internet Safety Rules to Stay Safe Online

Jeanne Meserve:
And we'll have other news from the business world when we return. Thanks for staying with us.

On Screen: VNN logo animated close

Script 2 (Length: 3-5 minutes): The story of a company under cyber attack unfolds over three days of news coverage. The CEO of Worldwide Global, Inc., the company under virtual siege, engages with VNN to detail key events of the attack and its impact on company operations and reputation.

On Screen: One month after the threat from The Void
VNN logo animated open.

For this and all scripts that follow, the "EXERCISE EXERCISE EXERCISE" watermark will be applied graphically, throughout.

On Screen [News Ticker]: Worldwide Global, Inc Under Virtual Siege

Jeanne Meserve:
I'm Jeanne Meserve, live from VNN headquarters in Washington, DC. After four weeks of threats from hacktivist network, The Void, it appears that today, their words have turned into action.

At a press conference this morning, Worldwide Global CEO Barton Ramsey announced that his company was under cyber siege, and that The Void was responsible.

Mr. Ramsey joins us live.

On Screen: Split screen or insert of live feed / interview appears: "Barton Ramsey, CEO Worldwide Global, Inc." as lower third appears on-screen to indicate this.

Jeanne Meserve:
Welcome to VNN, Mr. Ramsey.

Ramsey:
Thanks for having me on, Jeanne.

Jeanne Meserve:
First, you said today that Worldwide Global is under cyber attack. Can you give us more detail on the nature of that attack?

On Screen [News Ticker]: Breaking News
The Void Hacktivist Network Attacks Banking Accounts

Ramsey:
So far, we've seen The Void attack two aspects of our business. First, there was a failed attempt to transfer funds from one of our company accounts to an overseas bank by an unauthorized user. Our bank's security protocols questioned the validity of the transfer during the process and it was cancelled just minutes prior to being activated.

Additionally, several of our valued overseas clients in Europe and Asia received false invoices today. It seems that the hackers manipulated our systems and sent them.

Jeanne Meserve:
You said today, Mr. Ramsey, that The Void was responsible. How exactly do you know that?

On Screen [News Ticker]: Breaking News
Cyber Security Analysis Points to The Void

Ramsey:
Well, we combined the resources of our internal security team with two cyber security specialty firms.

Together, they were able to analyze the code that was inserted into our systems. When they took a look at it, the code had several signature-like elements to it that have been seen from The Void in the past.

Jeanne Meserve:
Was this a "zero-day" attack? Meaning, did this attack expose security issues you didn't even know existed?

On Screen [News Ticker]: Breaking News
"Zero-Day" Attack Exposed Unknown Security Issues

Ramsey:
I can say, Jeanne, that if we knew any flaws existed, we would have patched them immediately. We have a sterling security record until today, and we will get back on track.
AND we will do our best to see that these criminals pay for what they've done.

Jeanne Meserve:
Thanks for joining us, Mr. Ramsey.

Ramsey:
Thank you, Jeanne.

TEXT FADES IN FROM BLACK:
One week after the first attack…

On Screen [News Ticker]: Breaking News
More Cyber Attacks on Worldwide Global, Inc.

Jeanne Meserve:
Turning first to business news, it appears that there were more cyber attacks on Worldwide Global this morning.

This time, the hacktivist network The Void is openly claiming responsibility and acknowledging that this is a follow-up to their actions one week ago.

Here's how the attack unfolded:
At 9AM, all employees of Worldwide Global received emails from The Void that were masked so they appeared to come from an email address within the company.

On Screen [News Ticker]: Breaking News
The Void has Infiltrated Company's Internal Communications Systems

This indicates that The Void has infiltrated the company's internal communications systems and has some control over activities like creating, and possibly deleting, company email accounts.

At noon, the company's public-facing Web site began to slow down.

By 1PM it wasn't functioning at all…because The Void had inundated the company servers that pushed the site to millions of customers.

Just before we came on the air, we received notice that CEO Barton Ramsey had released the following statement, and I quote:

On Screen [Image]: Photo of Barton Ramsey with text from quote

"Today has been a trying day for Worldwide Global. In addition to the two cyber attacks, I am sorry to share that we are receiving extortion threats from The Void. They are threatening to release sensitive company information unless we give in to their demands. I want to make it clear to these perpetrators, as well as our employees, customers and stakeholders – we will not be doing so."

On Screen [News Ticker]: Breaking News
Worldwide Global is Receiving Extortion Threats from The Void
At this time it is not clear what type of information The Void may have or what demands it has made. But this is certainly another in a series of trying days for Worldwide Global and its CEO.

TEXT FADES IN FROM BLACK:
Three weeks after the first attack…

On Screen: Split screen or insert of live feed / interview appears: "Barton Ramsey, CEO Worldwide Global, Inc." as lower third appears on-screen to indicate this.

Jeanne Meserve:
Welcome again, Mr. Ramsey.

Ramsey:
Thanks for having me back, Jeanne.

Jeanne Meserve:
With Worldwide Global stocks continuing to tumble and multiple investigations now underway into the cyber attacks on your company, I hear there's some good news today?

On Screen [News Ticker]: Breaking News
Worldwide Global Stocks Tumbling and Multiple Investigations Underway

Ramsey:
Yes, Jeanne, of course we're not happy any of this occurred and we continue to engage with law enforcement and cyber security specialists looking into every aspect of how this happened, but we are relieved to say that we are rid of The Void.

Jeanne Meserve:
You are rid of The Void? What do you mean?

On Screen [News Ticker]: Breaking News
Company Intranet Page Replaced with Message from The Void

Ramsey:
Well, at about 3PM today, our company intranet page was replaced with a simple message from The Void that read, “It’s over. But don’t forget that we’re always watching.” We are confident that this is a direct result of the efforts I just mentioned, including working with law enforcement and bolstering our security efforts.

Jeanne Meserve:
So they hacked into your intranet to wave the white flag?

On Screen [News Ticker]: Breaking News
Company Aims to Prosecute The Void to the Fullest Extent of the Law

Ramsey:
Yes Jeanne, where some people see tongue in cheek humor, others see crimes, and we are working with those others to get to a point where we can prosecute The Void to the fullest extent of the law.

On Screen: Picture shown of phishing email

Jeanne Meserve:
Mr. Ramsey, it was reported today that Worldwide Global employees received phishing emails like those seen here a little over a month ago, and that this was one way that The Void exploited your security flaws.

On Screen [News Ticker]: Breaking News
CEO Confirms Phishing Emails Were Used by The Void

Ramsey:
I really can’t comment on the validity of the emails you’re presenting here, but I will confirm that phishing emails were used by The Void, yes.

What I want to emphasize, though, is that I’m just relieved to get on with business, and to re-engage with our customers, everywhere. Over the past two months, shifting focus to cyber terrorism became necessary for me, but now that we’ve taken care of The Void, my full focus is back to what we all do best, and that’s serving our clientele.

Jeanne Meserve:
Well, Mr. Ramsey, we wish you the best in those efforts.

Ramsey:
Thank you, Jeanne.

On Screen [News Ticker]: Up Next: News in Action Series
How Small Businesses Can Improve Cyber Security Employee Training

Jeanne Meserve:
And when we return, we’ll take a look at how small businesses can improve their cyber security employee training with an installment of our News In Action Series.

Until then, stay tuned in right here with VNN.

On Screen: VNN logo animated close.

Script 3 (Length: 3-5 minutes): This VNN Special Report is focused on the fallout from The Void's hack of Worldwide Global Inc.'s systems—what the attacks have meant to the company in hard numbers and reputation along with analysis from a cyber security expert who highlights best-practice methods of prevention.

On Screen: VNN logo animated open.

For this and all scripts that follow, the "EXERCISE EXERCISE EXERCISE" watermark will be applied graphically, throughout.

On Screen [Image]: Image of Barton Ramsey, with text overlay: RAMSEY RESIGNS!

Jeanne Meserve:
Welcome to VNN from our news headquarters in the nation's capital. Today Worldwide Global CEO Barton Ramsey resigned, after a series of cyber attacks on his company. Tonight: a special report.

On Screen [News Ticker]: Breaking News
Worldwide Global CEO Resigns in Aftermath of "Zero Day" Attacks

Jeanne Meserve:
It was nearly nine weeks ago that we first heard of the hacktivist network The Void**'s** plan to engage in what they called "extreme action against U.S. interests" in the form of a cyber attack. Five weeks later we learned that the target of the attacks was Worldwide Global.

On Screen [News Ticker]: Breaking News
Combined Efforts Stop Multiple Days of Relentless Cyber Attacks by The Void

Over several days, relentless attacks by The Void resulted in financial system breaches, extortion attempts, internal communications breaches, false invoicing, an inundation of the company's server that disabled its Web site, and more.

And it took the combined efforts of Worldwide Global, law enforcement and two cyber security specialty companies to stop them.

Tonight, we'll be discussing the fallout from these prolonged and devastating attacks with the founder of the Cyber Protection Initiative, Dr. Susan Lee-Hamilton.

On Screen [Image]: Split screen of Jeanne Meserve (left) and Dr. Susan Lee-Hamilton (right) with her name and title (Cyber Protection Initiative Founder) listed under photo. Headline reads, "Fallout from The Void's attack."

Jeanne Meserve:
First, Dr. Lee-Hamilton can you summarize the impact that this has had on Worldwide Global?

On Screen [News Ticker]: Breaking News
Worldwide Global Sales Down 15% From Projected Growth of 4%

Dr. Lee-Hamilton:

Well, in addition to the loss of the CEO, today, there has been a huge investor sell-off and devaluation of their stocks. This is really sad because they were such an up-and-coming company.

They went from being a small business to IPO status quickly and it seems that they didn't implement security advances to match their growing revenue streams.

Naturally their sales are down this quarter by 15 percent, when they were originally projected to grow about four percent. Layoffs have occurred as a result of all this financial stress, and of course, as of today, major leadership changes.

It just goes to show, whether you have one employee or 3,000, the stakes are the same in the end. If you ignore this, you risk losing something important, be it money or clients or employees.

Jeanne Meserve:
But this risk and these sorts of costs aren't limited to this one company, are they?

On Screen [News Ticker]: Breaking News
Median Cost of Cyber Crimes Per Year For a Company Rose to $5.9 Million in 2011

Dr. Lee-Hamilton:
No, not at all. In fact, recent studies by the Ponemon Institute—a research group that specializes in internet security—showed that the median cost of cyber crimes for a company per year rose to $5.9 million in 2011, up from $3.8 million in 2010.

Jeanne Meserve:
So let's backtrack from here and talk about causes—why did this happen?

On Screen [News Ticker]: Breaking News
Insider Events Led to The Void Gaining Access to Worldwide Global Systems

Dr. Lee-Hamilton:
Based on my understanding, there were several events that led to The Void being able to infiltrate.

First, there were some insider issues with a former employee who still had network access. He was discovered through a security audit, but by then it may have been too late.

Also, I've seen reports about a Void-created piece of hardware that was given to an unsuspecting employee. Once he or she installed it via their USB port, the damage was done.

And just before the attacks, I've also read reports about massive lags in network speed and network performance issues in several offices — things that indicate something's wrong.

Jeanne Meserve:
So a lot of that sounds like human error and not some science fiction or rocket science explanation.

On Screen [News Ticker]: Breaking News
Overlooked Warning Signs Could Have Prevented Critical Company Damage

Dr. Lee-Hamilton:
Exactly right, and that's why trainings and policies for employees are such an important part of a cyber security program.

Also, ensuring operating systems and security software are up to date is critical, as well as having what is called a "defense in depth" strategy. It's important to integrate all this into a plan and keep evolving and adapting the plan over time as your business grows.

Jeanne Meserve:
Well, given the statistics you laid out earlier, I understand why that approach is so important. Dr. Lee-Hamilton, thanks so much for joining us this evening.

Dr. Lee-Hamilton:
You're most welcome, Jeanne.

On Screen [News Ticker]: Up Next:
The Law Enforcement's Role in Investigating The Void's Crimes

Jeanne Meserve:
And when we return, we'll be discussing law enforcement's role with an agent involved in the ongoing investigation into this and other crimes from The Void.

On Screen: VNN logo animated close.