Practical Tabletop Drills for PSIRTS

FIRST PSIRT TC

Atlanta, Georgia, USA

27-28 February 2018

KRvW Associates, LLC

Ken van Wyk, ken@krvw.com, @KRvW

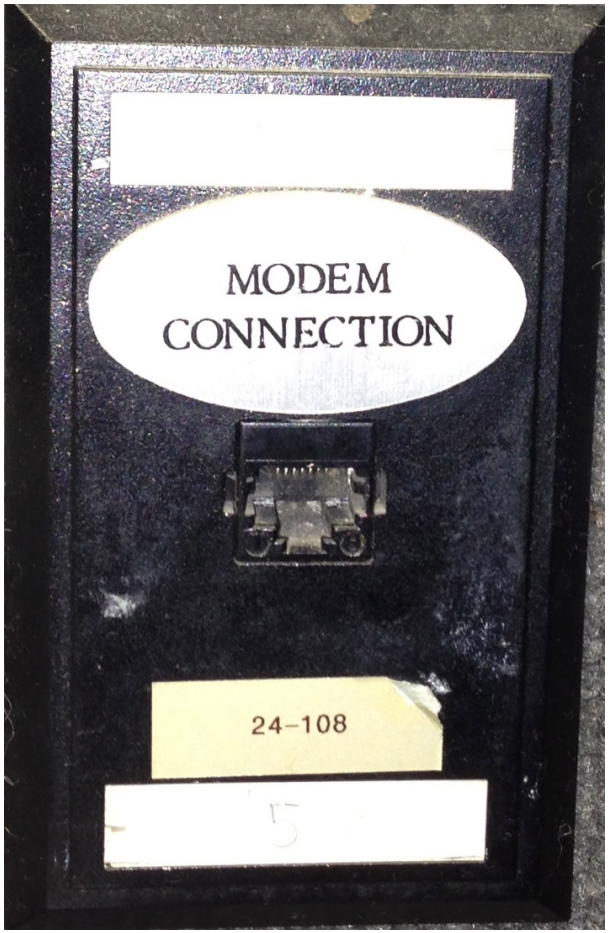
IRTs need to play with others

To name a few

- Human resources
- Communications
- Legal counsel
- Executive decision team
- Business owner
- Customers
- Government regulators
- And so on…

Technical excellence is not enough

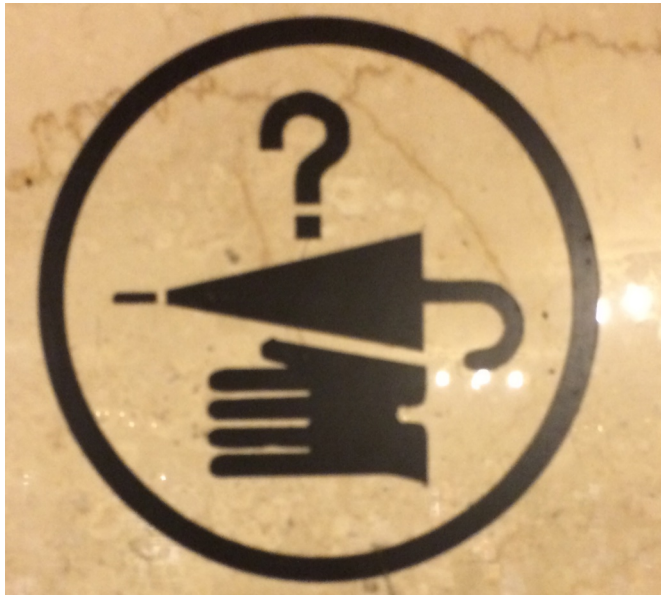
- You've hired a top-notch tech team
- You've purchased and are maintaining the best tools
- Your team is constantly abreast of the threat landscape
- These are great, but not enough



Consider this

Your success or failure may well be determined by matters outside your control

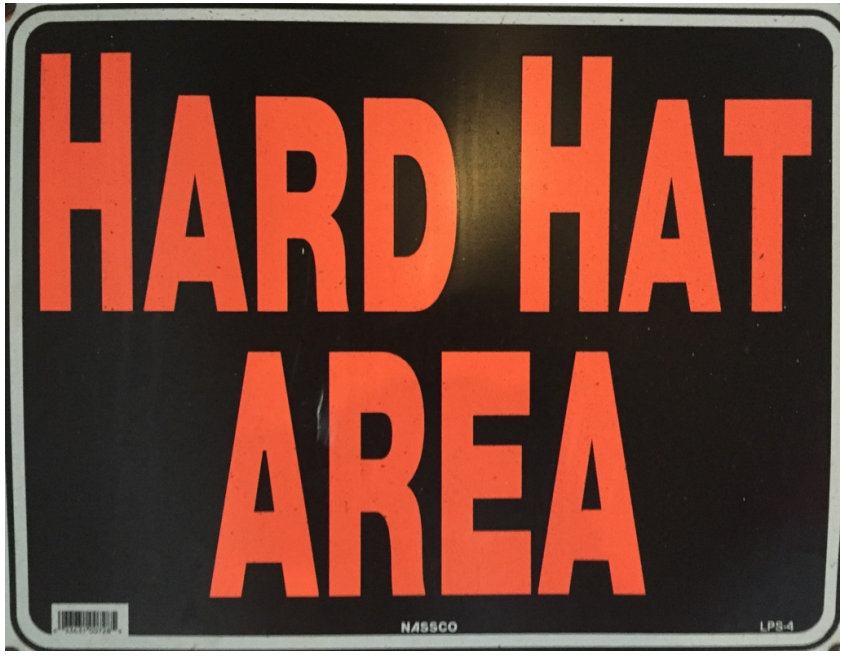
Now do you think they're all ready?



How do we prepare them?

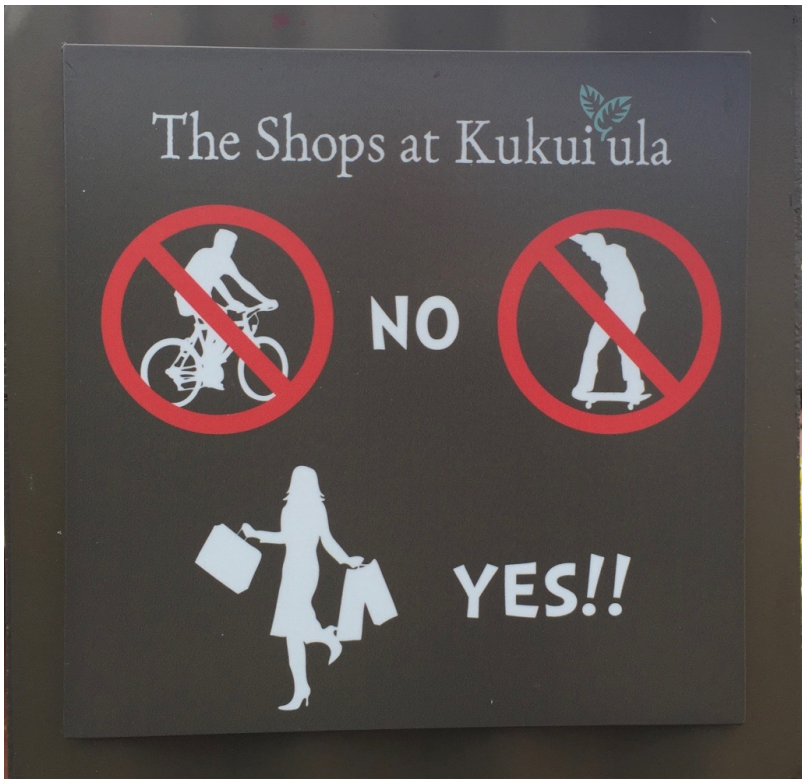
Three things you can work on

- Train the entire team
- Practice your processes
- Verify things are working how you want them to



Types of Drills

- Fully scripted
  - Announced
  - Events planned in detail
  - Tests process flow
- Hybrid (with twists)
  - Announced
  - Mostly scripted
  - Inject unexpected difficulties
  - Stresses process, communications, coordination
- Red/Blue team
  - Unannounced
  - Live



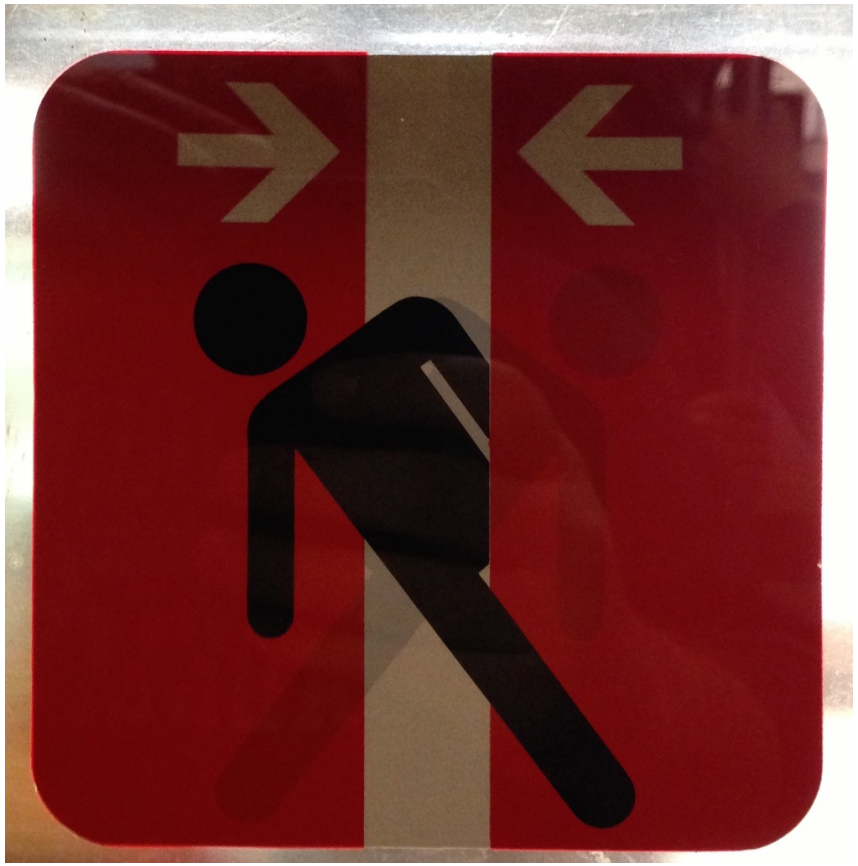
Keys to success

You will need

- All the key stakeholders
  - Leads or designees from each organization in the entire CSIRT plan
- A few realistic scenarios
  - Don’t forget the business
- A half day
- Facilitator
  - Best if facilitator isn’t a participant
- Planner
  - Someone to plan and write the scenarios

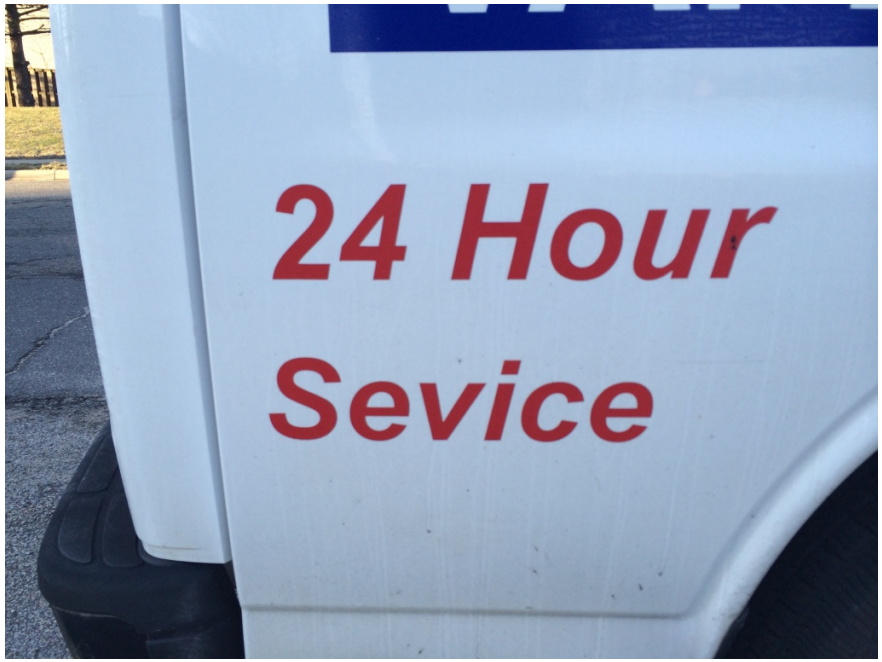
Planning the scenarios

- Considerations
  - Business nightmares
  - Involve the team to learn about the landscape
  - Don’t share the scenarios
- Each scenario should run for about an hour
- I generally build 3
  - 1 to practice (think: training)
  - 2 more to push the limits



Business nightmares

- Deep understanding of the business
  - Priorities and concerns
  - Strengths and weaknesses
- Now, what are the technical shortcomings
  - Signature-based protections
  - Business hour monitoring
  - Not everything monitored
- Limit sharing of scenarios



Hands-on time

Fictitious company

Let’s have some fun and see first-hand how this works

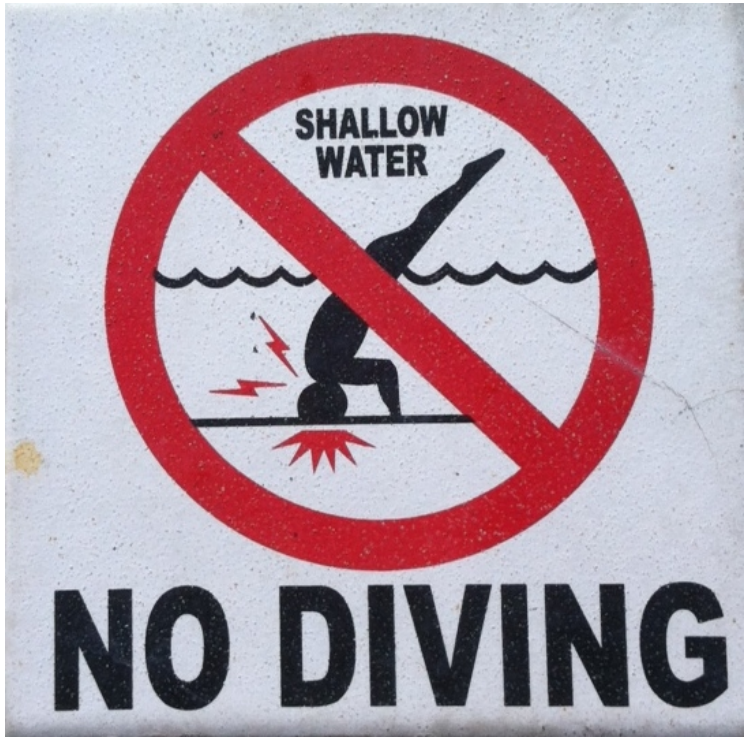
We’ll need some volunteers…

Setting the stage

- Introductions and key roles
- Facilitator - Ken van Wyk
  - I'll guide and "navigate" us during the exercise
  - I won't steer your responses
  - But I will keep us on task
- Players - All of you will emulate the roles we'll provide for you in a few minutes

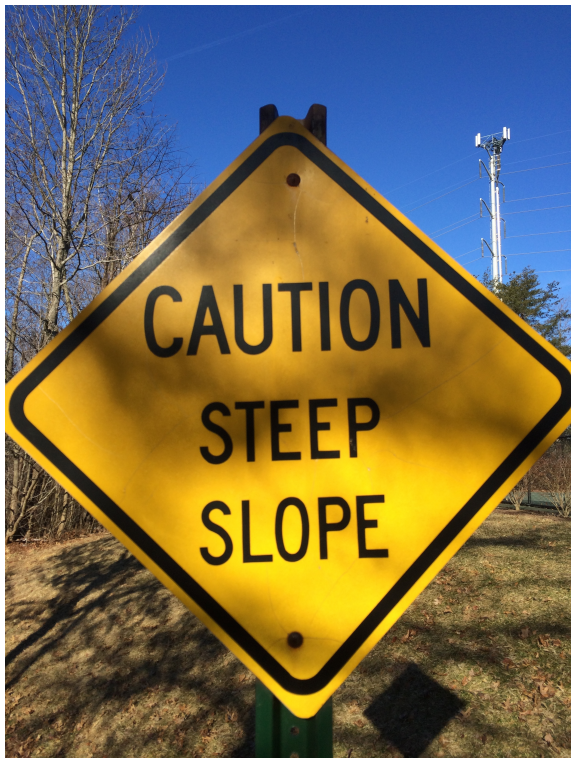
The exercises

- Cybersecurity emergency preparedness
  - Each scenario will follow a real-time schedule, but we will condense that for the exercise
  - The details are intended to be realistic to our fictitious company's environment



Rules

- Entirely constructive
  - We will explore your emergency preparedness
  - Our goal is not to fault anyone or anything
  - Our goal is to help you improve
- Questions
  - Please keep things realistic
  - Ask questions that you would during a live incident
  - Please keep non-operational questions until after we finish



Safe assumptions

- We're not trying to trick anyone
  - Take the information provided at face value
- Scenario is fictional but plausible
- Everyone here learns what is going on
  - But that won't necessarily be the case for a real incident
  - Consider communications realistically
- Complications may be inserted from time to time

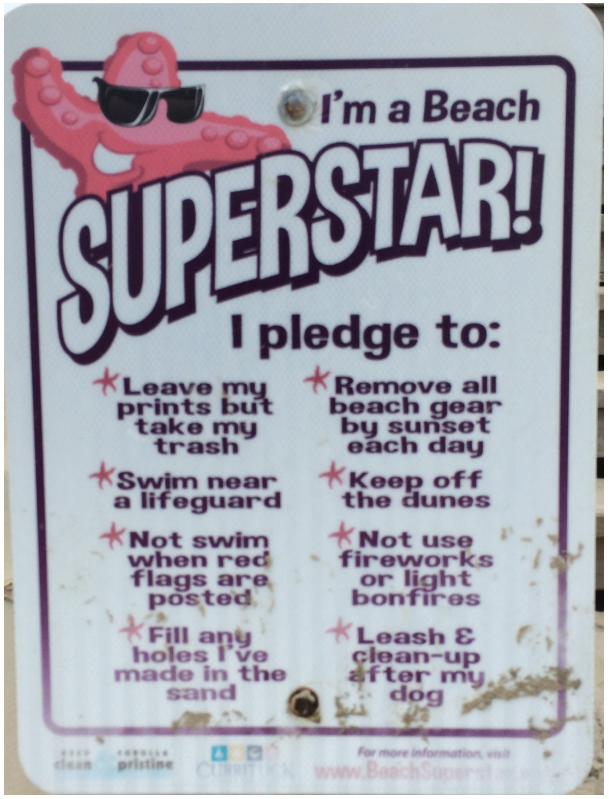
Process

I will introduce the events (aka “injects”) as they occur, along with timeline

- Basic data will be on slides

You respond as you would expect to

- Discuss process
- Ask operational questions
- Take actions as appropriate



Our company - *Meows The Time*

- In business for 5 years
- New market leader in IoT products
- IoT devices include
  - Security cameras, sensors
  - Thermostats
  - Home automation
  - Speakers / digital assistants
- US$1.5B in annual sales, including SaaS services
  - 10 million paying subscribers
  - Publicly traded on NASDAQ

Additional company details

- 500 employees
  - Engineering team in Silicon valley
  - Manufacturing in China
  - Customer support in Bangalore
- First product launch took the market by storm
- Latest feature set in 2nd generation products includes speaker interface
  - Speaker devices resulted from company acquisition 2 years ago

Product details

- Version 1 was grad school project brainchild of company CTO, Dudley Bobblefock
  - Prototype built on Raspberry Pi platform
  - Kernel is Linux, services via Java app on Tomcat app container
  - Launched commercial offering via GoFundMe page
- Devices connect via home WiFi or wired net, as well as Zigbee (home automation)
- Subscription service
  - Software updates
  - Remote access to security services

Additional product details

- Cloud services
  - Security alert monitoring
  - All built on REST APIs over latest TLS 1.2
  - Backend deployed on popular commercial cloud service
- Product engineering team is working on third generation product line
  - Scheduled to be rolled out in 2 months
  - Since updates are pushed, 2nd generation products will be phased out almost over night

Company PSIRT

- New business function, added after recent audit
- PSIRT manager hired 3 months ago
- PSIRT engineer added 1 month ago
- Board insisted on building PSIRT with world class talent
  - Hired PSIRT manager after lengthy search using company headhunter
  - Manager is a “rock star” IR techie, snatched from a major OS vendor’s own CSIRT

Roles

PSIRT Manager
PSIRT Engineer
Information Tech
General Counsel
Public Relations
Investor Relations
Engineering

Sales
Gov Relations
Support
Big Scary Customer
Small Customer
Government Customer
Journalist

Time - 09:00 (EST)

It’s early Wednesday morning, and things appear to be mostly “business as usual” at *Meows The Time*.

PSIRT reviews threat intelligence from past 24 hours

- A handful product security advisories published on Linux-related products, including: Apache Tomcat, NTP protocol design flaw, Dovecot IMAP server

Time - 10:00

Several popular security blog sites post details on NTP vulnerability

- Quickly gets dubbed the “Daylight Saving of Death” or DSoD vulnerability
  - Provisionally assigned a CVSS score of 6.5 and a new CVE number
  - CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
- Allows maliciously constructed NTP packet to run arbitrary code on any NTP client via buffer overrun caused by integer mishandling in NTP’s C code
  - Offending code module is in the parsing of timezone data
- One blogger publishes a short proof of concept code snippet that illustrates attack vector
  - Names his PoC code “The NyQuil Vector”
  - Runs a small “hello world” in affected NTP daemon process, logs to syslog

Time - 12:00

News media starts noticing the DDoS vulnerability and blogger's NyQuil Vector PoC code

National news outlets publish televised interviews with blogger who wrote the PoC

Time - 13:00

Product Support receives numerous phone calls asking if Meow products are affected by DSoD or NyQuil Vector

Big Scary Customer calls Support specifically

- They know Meow products evolved from Linux prototype
- Wants official company position on these vulnerabilities

Time - 10:00 (day 2)

- Media interviews have hit a fever pace as DSoD and NyQuil have gotten massive attention
- Dozens of software companies release their own product updates that roll out NTP patches
  - Bundled in with Tomcat and Dovecot patches
- Many of the software companies suggest that customers install patches ASAP

Time - 11:00

Product Support continues to receive calls about DSoD and NyQuil

PSIRT also receives dozens of emails asking if Meow is affected and, if so, when a fix will be released

Time - 16:00

- Product Engineering learns that DSoD affects Meow's security devices
  - Not developed by Meow internally
  - Acquired for Gen2 launch 2 years ago
- Provides a quick patch that blocks NyQuil PoC code from working
- Engineering informs Meow's PSIRT in an email

Time - 07:00 (Day 3)

Product Support receives calls from dozens of Meow customers, all saying:

Meow security alarms going off

Unable to disarm the alarm using iPhone or Android app

Notification on smart phone client saying

- "You've been hit by the Shenanigans Virus! If you want your alarm to be turned off, pay US$1000 in Bitcoin to DreadPirate@buttercup.org and you'll receive an antidote to be run on your PC. If you fail to pay up, your Meow security videos will be posted to Wikileaks later today. Have a nice day."

Time - 08:00

PSIRT receives via a threat intelligence partner a binary image copy of the Shenanigans Virus

Time - 10:00

Product Engineering sheepishly tells PSIRT the quick patch they built doesn't work with Shenanigans Virus

"Oh, by the way…"

As deployed on our Gen2 device, this vulnerability has a CVSS score of 8.8, since the Gen2 products run NTP as root

- CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

NTP in Gen2 is based on "ancient" version

- Will require significant changes to update to current NTP
- Publicly available NTP patches will not work for us

Will need time to test…

Time - 10:30

- Public Relations starts fielding dozens of media inquiries
  - All seeking on-camera statements
- Journalist calls Public Relations and asks for an official statement

Time - 11:00

Big Customer calls Product Support demanding answers

Small Customer calls Product Support demanding answers

Government Customer calls Product Support demanding answers

Time - 14:00

Product Engineering informs PSIRT they have a new patch available

"Should we push it out immediately?"

Time - 14:30

- Media reports start being published
- One report on a national media outlet quotes an unnamed Meow company employee
  - “We didn’t think we were affected by the NTP vulnerability announced a few days ago, but we were wrong.”
- General Counsel demands that Public Relations find out who the anonymous employee was

Time - 15:00

- So far today, Support has fielded over 2400 phone calls from irate customers
  - Their manager calls PSIRT to discuss the vulnerability and find out what they should tell customers

Time - 15:30

Meow's executive team tells PSIRT Manager they expect a patch will be rolled out "before close of business today"

Time - 16:00

What happens next?

How does the patch get rolled out?

Who tests the patch?

How?

Hot wash time

How did the team do?

What did they do well?

What mistakes did they make?

What systemic changes should they implement after this incident?

Kenneth R. van Wyk
KRvW Associates, LLC

Ken@KRvW.com
http://www.KRvW.com