

Who are these clowns?

Combined, your presenters have more than 40 years of Development, Enterprise Operations, Support, and Security experience most major industries: Retail, Legal, Medical, Financial, Insurance, Manufacturing, & Technology.

These guys currently work to secure free software.



Dave Russo
Principal Program Manager
Red Hat Inc.

CRob
Cat Herder
Red Hat Inc.



Your mission, should you choose to accept it, is to **participate** in an interactive **mock** disaster.

You are **equipped** with your wits, your experiences, and the assistance of the ladies and gentlemen surrounding you here in the room today.

BUT... to those **lucky** few who **DO** survive.... fabulous riches and fame beyond your wildest dreams await you at the turn of the page..... (We were rooting for you all along!)

You all will be faced with many difficult, yet **exciting** choices.

We're going to be honest here..... most of you aren't going to make it. Sorry, it's just that **MATH** is against you. Thanks for coming today. (We knew they'd never get through....seriously...just look at them.)



ZOMG! Where are the SERVERS?!?!

It is bright and early Monday morning. It started off like every other normal day. No one plans to have a bad day, but they sometimes happen. After entering the datacenter you gasp in horror! The server racks are empty! What do you do?

Race around in a panic!



[Go to Page 200](#)

Call Physical Security!



[Go to Page 98](#)

Oh wait, we moved all our servers to the cloud last week

[Go to Page 25](#)





200

Great job! Very impressive! You have a bright future ahead of you as you start your first day of a new job search after you're walked out of the building. Go back to [Page 1](#) and start over.





98

Your partners in physical security immediately leap to action. One mentions “We did have an alarm on an open door down in the underbasement. Want to join me and check it out?

Turn to [Page 67](#)



67



Going to the underbasement was a poor choice.

Your legend will live on in tales around the water cooler for days to come.

Go back to [Page 1](#) and start over.

>It is pitch black.

>You are likely to be eaten by a grue.

JOANNA'S CHEEZBURGER.COM ☺ ☺ ☺





The cloud is a lie!!! It's just some dude's garage!!! Go back to Page 1 and start over. Hahahahaha... just kidding.



25

With your missing server problem sorted out, you hurry off to your first meeting of the day: BUDGETING! (yay!) Turn to the next page



You have to also present to the Board later today....
what was it again your company does?

We're a funky-fresh start-up looking to revolutionize the world of savings for millenials and also fix all of our society's healthcare issues. Part bank, part hospital...all awesome. Opening new coffee-shop venture. [Welcome to Hospital Bank & Roastery \(est. 2018\)](#)



We write and maintain DYNAMIC CLOUD-BASED SYNERGISTIC SOFTWARE that OPTIMIZES our clients' lives by CLOUDIFYING their CLOUDS!! Our APIs are dead-sexy! [myFace](#) (specializes in pictures of people wearing clothes with their faces on it)



HoBank & Roastery Corporate Profile for Dave & CRob

we do this well

- reacting to our customers

we do this poorly

- long term planning

we REALLY care about THIS

- patient care & a delicious cup -o- joe



THREATS

regulation
IoT
safety/privacy

cryptolocker DAY3

wifi-enabled espresso machine DAY1

celebrity patient PII leaked DAY2

malicious insider (superman3/office space)



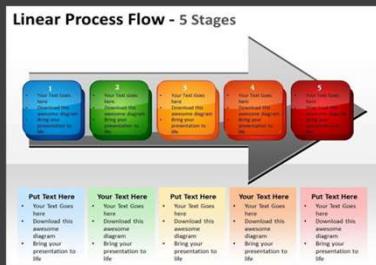


How should you allocate your security budget?

We'll spend our budget on the best PEOPLE!



[Go to Page 7](#)



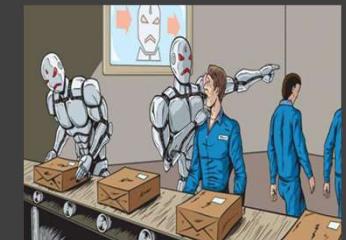
We'll spend our budget acquiring the best TECHNOLOGY



[Go to Page 79](#)



We'll spend our budget on developing the best PROCESSES



CLOUDSTRONG! Corporate Profile for Dave & CRob

we do this well

THREATS

bad code/no scanning

data breach in one subsystem that allows cross-infra access

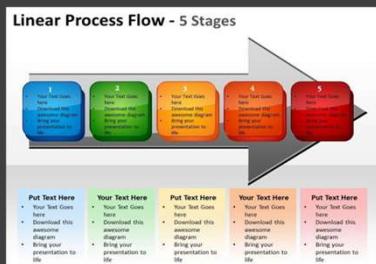
data sovereignty

we do this poorly

we REALLY care about THIS

my face How should you allocate your security budget?

We'll spend our budget on the best PEOPLE!



We'll spend our budget acquiring the best TECHNOLOGY



[Go to Page 17](#)



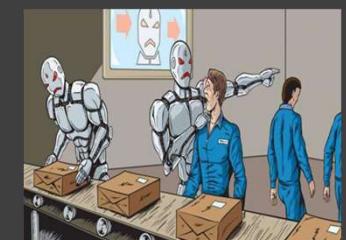
[Go to Page 1362](#)



[Go to Page 179](#)



We'll spend our budget on developing the best PROCESSES



Goober Corporate Profile for Dave & CRob

hi-tech, safety/privacy concerns,

we do this well

- engineering solutions; agile, fast delivery/fail fast

THREATS

volatile stocks

stunt hackers DAY1

regulation

Supply chain attack DAY 3

PII exposed DAY2

we do this poorly

we REALLY care about THIS

To Infinity And Beyond!

What Could Possibly Go Wrong?



GET A RIDE, ON COMMAND

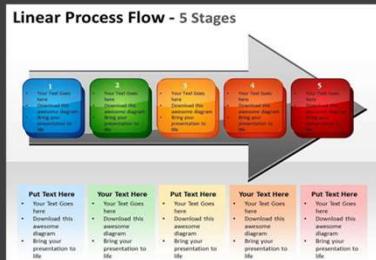
*Without the annoying driver with
the dubious background!*





How should you allocate your security budget?

We'll spend our budget on the best PEOPLE!



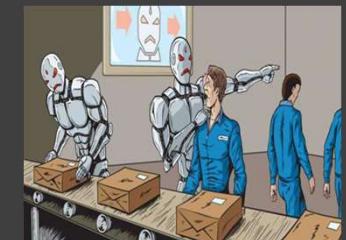
[Go to Page 27](#)



We'll spend our budget acquiring the best TECHNOLOGY



[Go to Page 279](#)





07

Day One



Founder Dr. Charles Manbun III, a homeopathic vegan brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PEOPLE are the future, so overwhelming funds finding the best and brightest people his espresso-stain dollars can buy.

CBO (Chief Barista Officer) Fran Cupwell has ordered some new espresso machines for the employee and patient cantinas. She is requesting network access for them.

Sounds GREAT! We LOVE the smell of freshly ground beans in the morning

Who doesn't love a good coffee? Offer to help her unbox and setup the new machines

Wait. Network wut?



[Go to Page 07](#)

[Go to Page 08](#)



[Go to Page 11](#)





Founder Dr. Charles Manbun III, a homeopathic vegan brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PROCESS is the key, so overwhelming funds finding the best and brightest checklists and processes his espresso-stain dollars can buy.

CBO (Chief Barista Officer) Fran Cupwell has ordered some new espresso machines for the employee and patient cantinas. She is requesting network access for them.

“We were meaning to talk to you about this...”



Go to [Page 96](#)



08

Day One



Founder Dr. Charles Manbun III, a homeopathic vegan brain surgeon, porkbelly futures maven, and coffee aficionado thinks that TECHNOLOGY is the future, so overwhelming funds finding the best and brightest TOOLS his espresso-stain dollars can buy.

CBO (Chief Barista Officer) Fran Cupwell has ordered some new espresso machines for the employee and patient cantinas. She is requesting network access for them.

The SOC analysts would like to talk to you



[Go to Page 44](#)

The CMDB manager wants to talk to you

[Go to Page 145](#)



The CBO wants to talk to you

[Go to Page 246](#)



79

Day One





42

Day One



Founder Dr. Churles Manbun III, a homeopathic vegan brain surgeon, porkbelly futures maven, and coffee aficionado thinks that a **BALANCED APPROACH** is the future, so he **SPLITS** his funding as **EQUALLY** as possible to ensure everyone gets a little something.

CBO (Chief Barista Officer) Fran Cupwell has ordered some new espresso machines for the employee and patient cantinas. She is requesting network access for them.

Race around in a panic!



[Go to Page 200](#)

Call Physical Security!

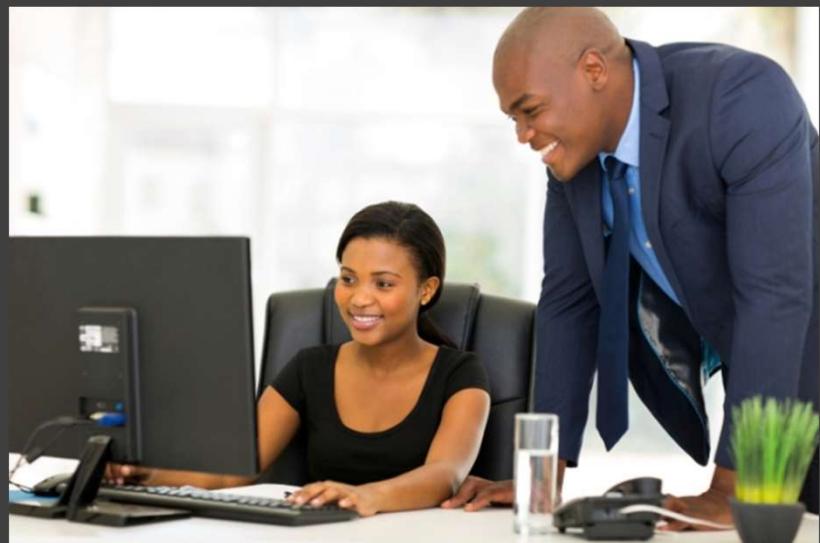


[Go to Page 98](#)

Oh wait, we moved all our servers to the cloud last week



[Go to Page 25](#)



Founder Tina Jones parlayed her small fortune from creation of the 2015 App Of the Year “Jump-rope!” into an online social media portal, collaboration hub, and cloud hosting provider.

Tina has assembled a large team of the best and brightest young DevSecOps people to help manage her **myFace** global infrastructure.

The SpiffyCloud Product Manager approaches you with concerns about an extremely high number of customer reported security defects in the latest release. What do you do?

“We’ll get right on that!” Refocus your people’s efforts to addressing the issues.

[Go to Page 26](#)



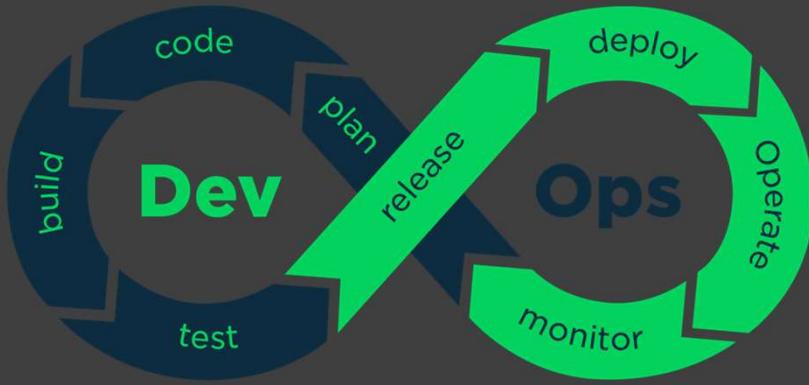
“Obviously the developers are doing it wrong.” We need to attack the root cause of the problem.

[Go to Page 27](#)



17

Day One



Founder Tina Jones parlayed her small fortune from creation of the 2015 App Of the Year “Jump-rope!” into an online social media portal, collaboration hub, and cloud hosting provider.

Tina has focused her budget on seasoned program managers to develop comprehensive processes that cover the full range of security events that may impact **myFace**'s business.

The SpiffyCloud Product Manager approaches you with concerns about an extremely high number of customer reported security defects in the latest release. What do you do?

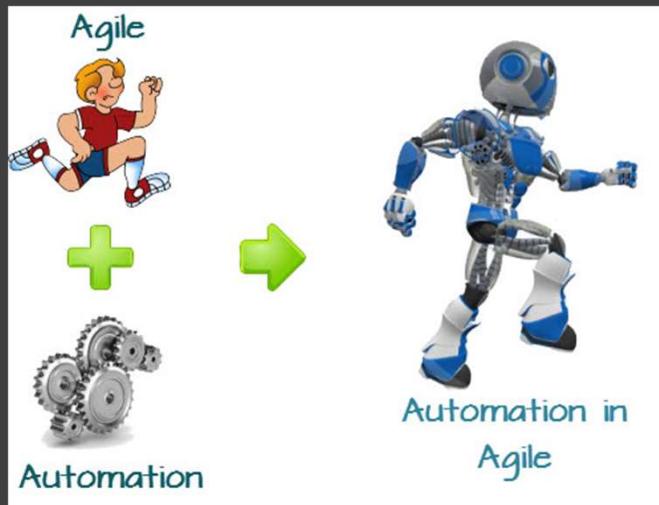
Obviously the developers are not following our robust SDLC - time for a training refresher!

According to our process flow we need to make some changes...



1362

Day One



Founder Tina Jones parlayed her small fortune from creation of the 2015 App Of the Year “Jump-rope!” into an online social media portal, collaboration hub, and cloud hosting provider.

Tina has committed the majority of her budget on building robust tools to automate the majority of **myFace**’s business flows and reduce the need for manpower.

The SpiffyCloud Product Manager approaches you with concerns about an extremely high number of customer reported security defects in the latest release. What do you do?

ZOMG! So many defect reports! False positives everywhere! We must analyze this info!

[Go to Page 34](#)



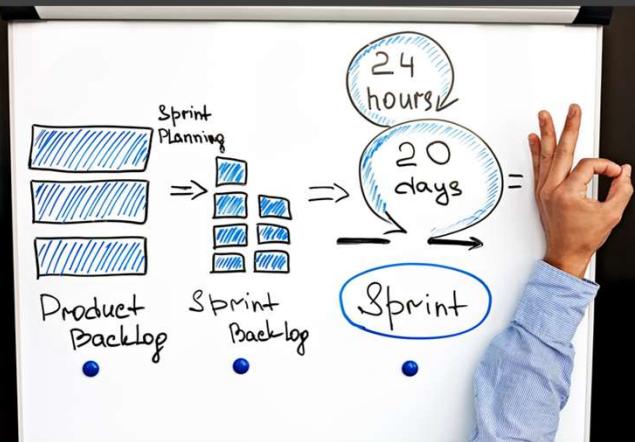
Our tooling couldn’t be wrong, these must be false negatives, exceptions and corner cases.

[Go to Page 35](#)



179

Day One



Founder Tina Jones parlayed her small fortune from creation of the 2015 App Of the Year “Jump-rope!” into an online social media portal, collaboration hub, and cloud hosting provider.

Tina has taken a balanced approach with the **myFace** budget in an attempt to provide at least minimal funding for people, processes and technology, although she is concerned that the resources may not be sufficient to cover the breadth of issues **myFace** might encounter.

The SpiffyCloud Product Manager approaches you with concerns about an extremely high number of customer reported security defects in the latest release. What do you do?

- Option 1  Go to Page xx
- Option 2  Go to Page xx
- Option 3  Go to Page XX

142

Day One



Undertaking a heroic effort, your army of people manage to power through the issues and address the customer concerns. However, the endless daily standups, status meetings and customer calls takes its toll and results in a reduction of morale and loss of focus on other priorities.

Tina is displeased and gives you a stern look every time she passes you in the hallway...

25

Day One

[Proceed to Day Two](#)



26

Day One



In a very productive meeting with the DevSecOps staff, you explain that the current situation is all their fault. However, the good news is that they have been identified as the root cause of the problem, and that it is your top priority to help resolve the gap in understanding so it won't happen again.

How do you accomplish this?

Throw some good old-fashioned instructorless compliance training at them.



[Go to Page 28](#)

Spend time teaching them the concepts of a secure development life cycle and supply chain.

[Go to Page 29](#)





Your noise cancelling headphones drown out the majority of the rage screams from down the hall after the compliance training is rolled out.

You leave the office thinking you have accomplished your goal, but the look on Tina's face when you see her in the parking lot makes you wonder...

27

Day One

[Proceed to Day Two](#)



SDLC



The DevSecOps staff seems to appreciate the time you spend reviewing information about secure development life cycle and supply chain with them over the next two weeks.

However, they seem to be distracted by other pressing tasks and you know that the upcoming release schedule will need to be adjusted. You are not convinced that a lot of what you have explained will get the necessary time and attention going forward.

28

Day One

[Proceed to Day Two](#)



Your noise cancelling headphones drown out the majority of the rage screams from down the hall after the compliance training is rolled out.

You leave the office thinking you have accomplished your goal, but the look on Tina's face when you see her in the parking lot makes you wonder...

30

Day One

[Proceed to Day Two](#)



In a very productive meeting where you thoroughly review the robust process documentation, you determine that the issues were caused by lack of resources and lack of tooling.

To address these deficiencies you can either re-focus everyone's efforts to addressing the issues at the expense of other tasks, or leave it be and handle it in the next sprint.

What do you do?

31

Day One

We're in this together! Everyone gets a list of issues to address - GO TEAM!!!

[Go to Page 32](#)



Have your lone project manager add copious notes to the To Do List for the next sprint.

[Go to Page 33](#)





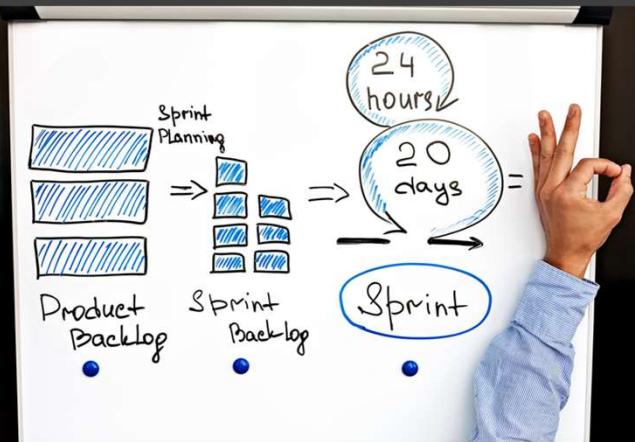
Undertaking a heroic effort, your small staff manages to follow the processes, power through the issues and address the customer concerns. However, the endless daily standups, status meetings and customer calls takes its toll and results in a reduction of morale and loss of focus on other priorities.

Tina is displeased and gives you a stern look every time she passes you in the hallway...

32

Day One

[Proceed to Day Two](#)



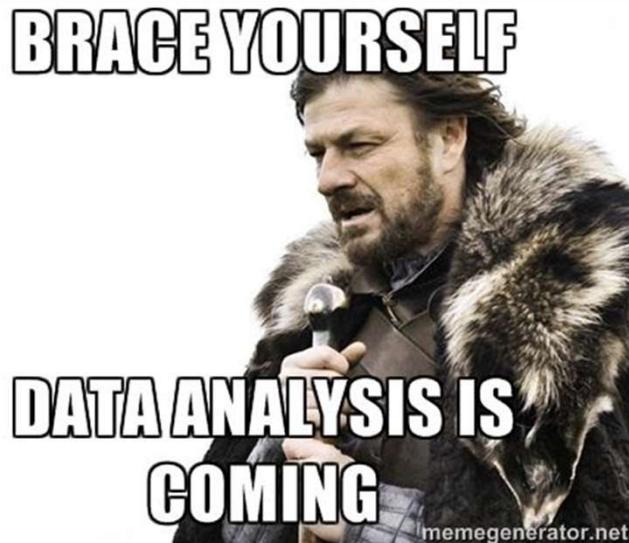
The project manager plugs the information into the plan for the upcoming sprint. However, he is skeptical that there are enough resources to address these changes so the scope of the work will need to be reduced.

Also, Tina is getting a lot of calls from unhappy customers. Each day she leaves a list of the customers who called her on your desk. Written in red pen...

33

Day One

[Proceed to Day Two](#)



The amount of data provided by your automation tools is daunting. With no one to oversee the automation in “real time” and no documented process for how to handle this, you will now have to backtrack through the information to determine what is an actual issue and what is not.

What do you do?

Just pass this over to the audit team, they can dig into it.

Get everyone together and have them step through the data, no matter how long it takes.

We don't have time for this now, push it to the next sprint.



[Go to Page 38](#)



[Go to Page 36](#)

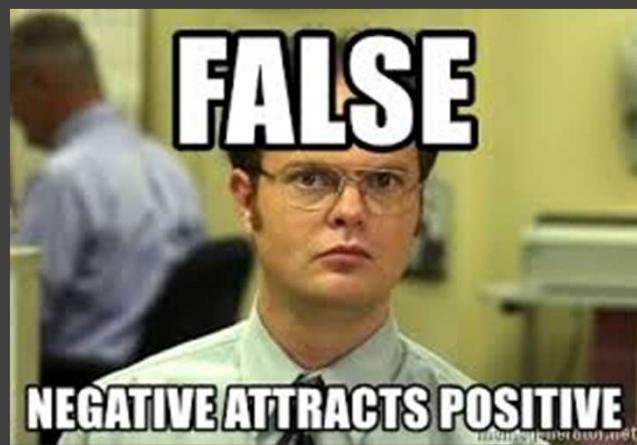


[Go to Page 37](#)



34

Day One



The awesomeness of the tooling is almost blinding, even if the associated processes are a bit of a grey area. You highly doubt the tools are wrong, and to review how they work will take a lot of time and effort from your very limited workforce.

Tina looks to you to decide how to handle the situation.

We better be sure and refocus our resources to double-check the tooling

We don't have the bandwidth or process understanding - trust the tooling and defer this to the next sprint.

[Go to Page 40](#)



[Go to Page 39](#)



35

Day One



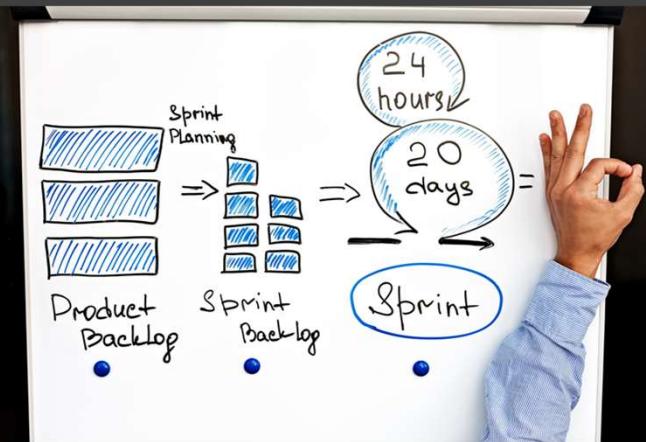
Undertaking a heroic effort, your army of people manage to review the defect reports, power through the issues and address the customer concerns. However, the endless daily standups, status meetings and customer calls takes its toll and results in a reduction of morale and loss of focus on other priorities.

Tina is displeased and gives you a stern look every time she passes you in the hallway...

36

Day One

[Proceed to Day Two](#)



The project manager plugs the information into the plan for the upcoming sprint. However, he is skeptical that there are enough resources to address these changes so the scope of the work will need to be reduced.

Also, Tina is getting a lot of calls from unhappy customers. Each day she leaves a list of the customers who called her on your desk. Written in red pen...

37

Day One

[Proceed to Day Two](#)



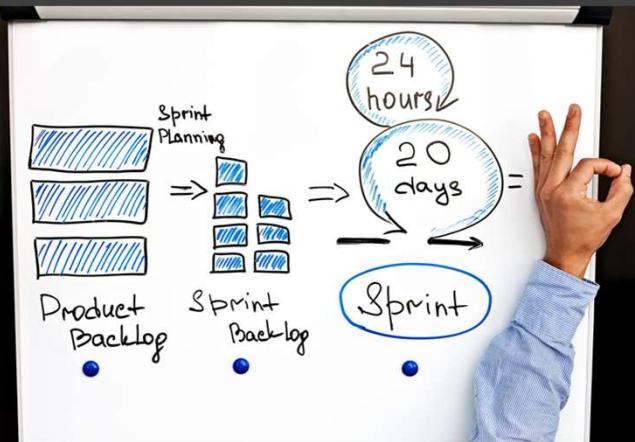
Your noise cancelling headphones drown out the majority of the rage screams from down the hall after the reports are given to the audit team to deal with.

You leave the office thinking you have accomplished your goal, but the look on Tina's face when you see her in the parking lot makes you wonder...

38

Day One

[Proceed to Day Two](#)



The project manager plugs the information into the plan for the upcoming sprint. However, he is skeptical that there are enough resources to address these changes so the scope of the work will need to be reduced.

Also, Tina is getting a lot of calls from unhappy customers. Each day she leaves a list of the customers who called her on your desk. Written in red pen...

39

Day One

[Proceed to Day Two](#)



Undertaking a heroic effort, your small staff manages to review the defect reports, power through the issues and address the customer concerns. However, the endless daily standups, status meetings and customer calls takes its toll and results in a reduction of morale and loss of focus on other priorities.

Tina is displeased and gives you a stern look every time she passes you in the hallway...

40

Day One

[Proceed to Day Two](#)



**YEAH, IF YOU COULD JUST GO
AHEAD AND PUT THAT IN THE
CLOUD**

memegenerator.net

During the morning leadership meeting Neil Bitsanbytes, the HDD (Head Data Dude) brings up an article from an insider technology website that is reporting several companies (including MyFace) are using Krazy Ivan's Cloud Service to store their customer data. Krazy Ivan has a server farm in Uzbleekistan, and the government of that country is negotiating to sell large blocks of it to various other entities.

Tina and Neil look at you expectantly...

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Under the laws of Uzbleekistan the government is allowed to do this.

ZOMG! We need to move our data to a new onshore cloud provider yesterday!!!

[Go to Page 50](#)



41

Day Two



**YEAH, IF YOU COULD JUST GO
AHEAD AND PUT THAT IN THE
CLOUD**

memegenerator.net

During the morning leadership meeting Neil Bitsanbytes, the HDD (Head Data Dude) brings up an article from an insider technology website that is reporting several companies (including MyFace) are using Krazy Ivan's Cloud Service to store their customer data. Krazy Ivan has a server farm in Uzbleekistan, and the government of that country is negotiating to sell large blocks of it to various other entities.

Tina and Neil look at you expectantly...

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Under the laws of Uzbleekistan the government is allowed to do this.

ZOMG! We need to move our data to a new onshore cloud provider yesterday!!!

[Go to Page 51](#)



42

Day Two



During the morning leadership meeting Neil Bitsanbytes, the HDD (Head Data Dude) brings up an article from an insider technology website that is reporting several companies (including MyFace) are using Krazy Ivan's Cloud Service to store their customer data. Krazy Ivan has a server farm in Uzbleekistan, and the government of that country is negotiating to sell large blocks of it to various other entities.

Tina and Neil look at you expectantly...

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Under the laws of Uzbleekistan the government is allowed to do this.

ZOMG! We need to move our data to a new onshore cloud provider yesterday!!!

[Go to Page 52](#)



43

Day Two



**YEAH, IF YOU COULD JUST GO
AHEAD AND PUT THAT IN THE
CLOUD**

memegenerator.net

During the morning leadership meeting Neil Bitsanbytes, the HDD (Head Data Dude) brings up an article from an insider technology website that is reporting several companies (including MyFace) are using Krazy Ivan's Cloud Service to store their customer data. Krazy Ivan has a server farm in Uzbleekistan, and the government of that country is negotiating to sell large blocks of it to various other entities.

Tina and Neil look at you expectantly...

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Under the laws of Uzbleekistan the government is allowed to do this.

ZOMG! We need to move our data to a new onshore cloud provider yesterday!!!

[Go to Page 53](#)



44

Day Two



**YEAH, IF YOU COULD JUST GO
AHEAD AND PUT THAT IN THE
CLOUD**

memegenerator.net

During the morning leadership meeting Neil Bitsanbytes, the HDD (Head Data Dude) brings up an article from an insider technology website that is reporting several companies (including MyFace) are using Krazy Ivan's Cloud Service to store their customer data. Krazy Ivan has a server farm in Uzbleekistan, and the government of that country is negotiating to sell large blocks of it to various other entities.

Tina and Neil look at you expectantly...

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Under the laws of Uzbleekistan the government is allowed to do this.

ZOMG! We need to move our data to a new onshore cloud provider yesterday!!!

[Go to Page 54](#)



45

Day Two



**YEAH, IF YOU COULD JUST GO
AHEAD AND PUT THAT IN THE
CLOUD**

memegenerator.net

During the morning leadership meeting Neil Bitsanbytes, the HDD (Head Data Dude) brings up an article from an insider technology website that is reporting several companies (including MyFace) are using Krazy Ivan's Cloud Service to store their customer data. Krazy Ivan has a server farm in Uzbleekistan, and the government of that country is negotiating to sell large blocks of it to various other entities.

Tina and Neil look at you expectantly...

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Under the laws of Uzbleekistan the government is allowed to do this.

ZOMG! We need to move our data to a new onshore cloud provider yesterday!!!

[Go to Page 55](#)



46

Day Two



**YEAH, IF YOU COULD JUST GO
AHEAD AND PUT THAT IN THE
CLOUD**

memegenerator.net

During the morning leadership meeting Neil Bitsanbytes, the HDD (Head Data Dude) brings up an article from an insider technology website that is reporting several companies (including MyFace) are using Krazy Ivan's Cloud Service to store their customer data. Krazy Ivan has a server farm in Uzbleekistan, and the government of that country is negotiating to sell large blocks of it to various other entities.

Tina and Neil look at you expectantly...

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Under the laws of Uzbleekistan the government is allowed to do this.

ZOMG! We need to move our data to a new onshore cloud provider yesterday!!!

[Go to Page 56](#)



47

Day Two



During the morning leadership meeting Neil Bitsanbytes, the HDD (Head Data Dude) brings up an article from an insider technology website that is reporting several companies (including MyFace) are using Krazy Ivan's Cloud Service to store their customer data. Krazy Ivan has a server farm in Uzbleekistan, and the government of that country is negotiating to sell large blocks of it to various other entities.

Tina and Neil look at you expectantly...

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Under the laws of Uzbleekistan the government is allowed to do this.

ZOMG! We need to move our data to a new onshore cloud provider yesterday!!!

[Go to Page 57](#)



48

Day Two



**YEAH, IF YOU COULD JUST GO
AHEAD AND PUT THAT IN THE
CLOUD**

memegenerator.net

During the morning leadership meeting Neil Bitsanbytes, the HDD (Head Data Dude) brings up an article from an insider technology website that is reporting several companies (including MyFace) are using Krazy Ivan's Cloud Service to store their customer data. Krazy Ivan has a server farm in Uzbleekistan, and the government of that country is negotiating to sell large blocks of it to various other entities.

Tina and Neil look at you expectantly...

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located. Under the laws of Uzbleekistan the government is allowed to do this.

ZOMG! We need to move our data to a new onshore cloud provider yesterday!!!

[Go to Page 58](#)



49

Day Two



ONE DOES NOT SIMPLY

MOVE TO A NEW DATACENTER

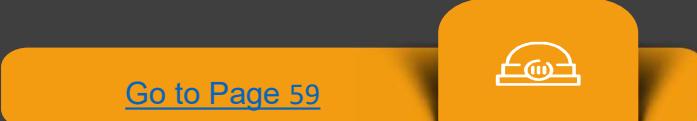
imgflip.com

Due to the amount of time you had spent working on the defects you were already behind schedule and your army of people were worn out. Fortunately for this problem you have the resources to perform the migration, but you struggle mightily due to not having a defined process in place nor tools to handle the majority of the gruntwork. At the end of the effort the team's morale is even lower and your schedules have been destroyed.

Take some time to re-prioritize the upcoming tasks



FULL SPEED AHEAD - press on and get caught up!!!



Re-focus some effort on internal improvements



As the phones ring off their hooks with angry customers, you rally the team to migrate your cloud data to a new provider.

Tina spends the majority of her time doing PR to buoy the company's image and assure the customers that the security of their data is the top priority.



50

Day Two



ONE DOES NOT SIMPLY

MOVE TO A NEW DATACENTER

imgflip.com

As the phones ring off their hooks with angry customers, you rally the team to migrate your cloud data to a new provider.

Tina spends the majority of her time doing PR to buoy the company's image and assure the customers that the security of their data is the top priority.

Fortunately for this problem you have the resources to perform the migration, but you struggle mightily due to not having a defined process in place nor tools to handle the majority of the gruntwork. The anger of the developers further hampers these efforts and several key people leave in disgust. This will have implications beyond the current crisis...

Take some time to re-prioritize the upcoming tasks



FULL SPEED AHEAD - press on and get caught up!!!



Re-focus some effort on internal improvements



51

Day Two

ONE DOES NOT SIMPLY

MOVE TO A NEW DATACENTER

imgflip.com

As the phones ring off their hooks with angry customers, you rally the team to migrate your cloud data to a new provider.

Tina spends the majority of her time doing PR to buoy the company's image and assure the customers that the security of their data is the top priority.

Fortunately for this problem you have the resources to perform the migration, and the secure supply chain training helps offset some of the challenges of not having a defined process in place. However, the lack of tools to handle the majority of the gruntwork makes the effort slow and tedious. At the end of the effort the team's morale is even lower and your upcoming schedules all need to be reworked.

Take some time to re-prioritize the upcoming tasks



FULL SPEED AHEAD - press on and get caught up!!!



Re-focus some effort on internal improvements



52

Day Two



ONE DOES NOT SIMPLY



MOVE TO A NEW DATACENTER

imgflip.com

Due to the amount of time you had spent working on the defects you were already behind schedule and your team was worn out. Fortunately for this problem you have a process in place to address this sort of situation, but you struggle mightily due to not having the resources or tools to follow them and perform the actual tasks. After a long, tedious effort that is fraught with human error, the team's morale is even lower and your schedules have been destroyed.

Take some time to re-prioritize the upcoming tasks



FULL SPEED AHEAD - press on and get caught up!!!



Re-focus some effort on internal improvements



53

Day Two

ONE DOES NOT SIMPLY

MOVE TO A NEW DATACENTER

imgflip.com

As the phones ring off their hooks with angry customers, you rally the team to migrate your cloud data to a new provider.

Tina spends the majority of her time doing PR to buoy the company's image and assure the customers that the security of their data is the top priority.

Fortunately for this problem you have a process in place to address this sort of situation, but you struggle mightily due to not having enough resources to do the work nor tools to streamline it. The anger of the developers further hampers these efforts and several key people spontaneously combust under the strain. This will have implications beyond the current crisis...

Take some time to re-prioritize the upcoming tasks



FULL SPEED AHEAD - press on and get caught up!!!



Re-focus some effort on internal improvements



54

Day Two

ONE DOES NOT SIMPLY

MOVE TO A NEW DATACENTER

imgflip.com

Fortunately for this problem you have a process in place to address this sort of situation, but you struggle mightily due to not having enough resources to do the work nor tools to streamline it. On top of this, the process changes and tasks you had deferred to the next sprint are happening at the same time, which causes a lot of confusion and strained nerves. People are starting to draw moustaches, glasses and angry eyebrows on each others' shirts in their anger!

Take some time to re-prioritize the upcoming tasks



FULL SPEED AHEAD - press on and get caught up!!!



Re-focus some effort on internal improvements



As the phones ring off their hooks with angry customers, you rally the team to migrate your cloud data to a new provider.

Tina spends the majority of her time doing PR to buoy the company's image and assure the customers that the security of their data is the top priority.



55

Day Two



ONE DOES NOT SIMPLY

MOVE TO A NEW DATACENTER

Fortunately for this problem you have tools that make the data migration easier, but you don't have enough resources to do it quickly and there is a lot of confusion without a process to guide them.

Take some time to re-prioritize the upcoming tasks



FULL SPEED AHEAD - press on and get caught up!!!



Re-focus some effort on internal improvements



As the phones ring off their hooks with angry customers, you rally the team to migrate your cloud data to a new provider.

Tina spends the majority of her time doing PR to buoy the company's image and assure the customers that the security of their data is the top priority.



56

Day Two



ONE DOES NOT SIMPLY

MOVE TO A NEW DATACENTER

Fortunately for this problem you have tools that make the data migration easier, but you don't have enough resources to do it quickly and there is a lot of confusion without a process to guide them. The anger of the audit team further hampers these efforts and several key people spontaneously combust under the strain. This will have implications beyond the current crisis...

Take some time to re-prioritize the upcoming tasks



FULL SPEED AHEAD - press on and get caught up!!!



Re-focus some effort on internal improvements



As the phones ring off their hooks with angry customers, you rally the team to migrate your cloud data to a new provider.

Tina spends the majority of her time doing PR to buoy the company's image and assure the customers that the security of their data is the top priority.



57

Day Two

ONE DOES NOT SIMPLY

MOVE TO A NEW DATACENTER

imgflip.com

Fortunately for this problem you have tools that make the data migration easier, but you don't have enough resources to do it quickly and there is a lot of confusion without a process to guide them. On top of this, the tooling changes and tasks you had deferred to the next sprint are happening at the same time, which causes a lot of confusion and strained nerves. People are starting to draw moustaches, glasses and angry eyebrows on each others' shirts in their anger!

Take some time to re-prioritize the upcoming tasks



FULL SPEED AHEAD - press on and get caught up!!!



Re-focus some effort on internal improvements



58

Day Two



59



Historians may one day liken the team's reaction to your directives to the sacking of Rome. Tina is very disappointed in your draconian expectations, and encourages you to start the next phase of your career.

Go back to [Page 50](#) and try again.



60



Historians may one day liken the team's reaction to your directives to the sacking of Rome. Tina is very disappointed in your draconian expectations, and encourages you to start the next phase of your career.

Go back to [Page 51](#) and try again.



61



Historians may one day liken the team's reaction to your directives to the sacking of Rome. Tina is very disappointed in your draconian expectations, and encourages you to start the next phase of your career.

Go back to [Page 52](#) and try again.



62



Historians may one day liken the team's reaction to your directives to the sacking of Rome. Tina is very disappointed in your draconian expectations, and encourages you to start the next phase of your career.

Go back to [Page 53](#) and try again.



63



Historians may one day liken the team's reaction to your directives to the sacking of Rome. Tina is very disappointed in your draconian expectations, and encourages you to start the next phase of your career.

Go back to [Page 54](#) and try again.



64



Historians may one day liken the team's reaction to your directives to the sacking of Rome. Tina is very disappointed in your draconian expectations, and encourages you to start the next phase of your career.

Go back to [Page 55](#) and try again.



65



Historians may one day liken the team's reaction to your directives to the sacking of Rome. Tina is very disappointed in your draconian expectations, and encourages you to start the next phase of your career.

Go back to [Page 56](#) and try again.



66



Historians may one day liken the team's reaction to your directives to the sacking of Rome. Tina is very disappointed in your draconian expectations, and encourages you to start the next phase of your career.

Go back to [Page 57](#) and try again.



67



Historians may one day liken the team's reaction to your directives to the sacking of Rome. Tina is very disappointed in your draconian expectations, and encourages you to start the next phase of your career.

Go back to [Page 58](#) and try again.



You meet with the team and take a look at the current task list, the (now invalid) timelines and where you are behind schedule.

With the help of Gertrude Gantchart, the premier myFace project manager, you adjust the schedule and the deliverables so you won't be working your awesome team into the pit of insanity and despair.

Tina is disappointed with the delays, but pleased that the team appears happy with the more realistic expectations.



68

Day Two

[Proceed to Day Three](#)



You meet with the team and take a look at the current task list, the (now invalid) timelines and where you are behind schedule.

With the help of Gertrude Gantchart, the premier myFace project manager, you adjust the schedule and the deliverables so you won't be working your awesome team into the pit of insanity and despair and will likely avoid an open rebellion.

Tina is disappointed with the delays, but pleased that the team appears happy with the more realistic expectations and are no longer trying to burn down the building.



69

Day Two

[Proceed to Day Three](#)



You meet with the team and take a look at the current task list, the (now invalid) timelines and where you are behind schedule.

With the help of Gertrude Gantchart, the premier myFace project manager, and your team's knowledge of SDLC you adjust the schedule and the deliverables so you won't be working your awesome team into the pit of insanity and despair.

Tina is disappointed with the delays, but pleased that the team appears happy with the more realistic expectations.



70

Day Two

[Proceed to Day Three](#)



You meet with Patricia Peterson to consult her *Binder Of All Things Process* to figure out how things should be reprioritized. The tasks are all significantly behind schedule and the whole thing needs reworked...

The two of you are able to adjust the schedule and the deliverables according to the defined processes so you won't be working your team into the pit of insanity and despair.

Tina is disappointed with the delays, but pleased that the team appears happy with the more realistic expectations.

[Proceed to Day Three](#)



71

Day Two



You meet with Patricia Peterson to consult her *Binder Of All Things Process* to figure out how things should be reprioritized. The tasks are all significantly behind schedule and the whole thing needs reworked...

The two of you are able to adjust the schedule and the deliverables according to the defined processes so you won't be working your team into the pit of insanity and despair and will likely avoid an open rebellion.

Tina is disappointed with the delays, but pleased that the team appears happy with the more realistic expectations and are no longer trying to burn down the building.



72

Day Two

[Proceed to Day Three](#)



You meet with Patricia Peterson to consult her *Binder Of All Things Process* to figure out how things should be reprioritized. The tasks are all significantly behind schedule and too many things have been added to upcoming sprints - the whole thing needs reworked...

The two of you are able to adjust the schedule and the deliverables according to the defined processes so you won't be working your team into the pit of insanity and despair. You hope.

Tina is disappointed with the scope reduction and delays, but pleased that the team appears happy with the more realistic expectations.



73

Day Two

[Proceed to Day Three](#)



You meet with Terrance Technophile, your tools guru, to review the work queue and upcoming schedule. The entire thing is in shambles and needs to be reworked.

With the help of his cool ProjectFixer 2000 application, you are able to adjust the schedule and the deliverables so you won't be working your team into the pit of insanity and despair.

Tina is disappointed with the delays, but pleased that the team appears happy with the more realistic expectations.



74

Day Two

[Proceed to Day Three](#)



You meet with Terrance Technophile, your tools guru, to review the work queue and upcoming schedule. The entire thing is in shambles and needs to be reworked.

Tina holds the door shut to prevent the angry audit team from storming the conference room while you use his cool ProjectFixer 2000 application to adjust the schedule and the deliverables so you won't be working your team into the pit of insanity and despair.

Tina is disappointed with the delays, but pleased that the team appears happy with the more realistic expectations and are no longer trying to burn down the building.



75

Day Two

[Proceed to Day Three](#)



You meet with Terrance Technophile, your tools guru, to review the work queue and upcoming schedule. The tasks are all significantly behind schedule and too many things have been added to upcoming sprints - the whole thing needs reworked...

With the help of his cool ProjectFixer 2000 application, you are able to adjust the schedule and the deliverables so you won't be working your team into the pit of insanity and despair.

Tina is disappointed with the delays, but pleased that the team appears happy with the more realistic expectations.

76

Day Two

[Proceed to Day Three](#)



77

Day Two

Hoping to be able to better handle the next crisis (this is called *Choose Your Own Disaster* after all) you decide to utilize the team to put some improvements into place with the processes and tooling that have proven insufficient recently.

This doesn't do anything to help your schedule issues, and Tina is not happy. She hopes that these improvements are worth the additional effort and focus they are getting...

[Proceed to Day Three](#)



78

Day Two

Hoping to be able to better handle the next crisis (this is called *Choose Your Own Disaster* after all) you decide to utilize the team to put some improvements into place with the processes and tooling that have proven insufficient recently.

This doesn't do anything to help your schedule issues, and Tina is not happy. She hopes that these improvements are worth the additional effort and focus they are getting, and have not further angered your staff...

[Proceed to Day Three](#)



79

Day Two

Hoping to be able to better handle the next crisis (this is called *Choose Your Own Disaster* after all) you decide to utilize the team to put some improvements into place with the processes and tooling that have proven insufficient recently.

This doesn't do anything to help your schedule issues, and Tina is not happy. She hopes that these improvements are worth the additional effort and focus they are getting, but is somewhat encouraged by the positive feedback she is getting from the staff...

[Proceed to Day Three](#)



80

Day Two

Hoping to be able to better handle the next crisis (this is called *Choose Your Own Disaster* after all) you decide to utilize the team to refine some of your processes and put some improvements into place with tooling that has proven insufficient recently.

This is difficult to do with your limited manpower and doesn't do anything to help your schedule issues, which makes Tina unhappy. She hopes that these improvements are worth the additional effort and focus they are getting...

[Proceed to Day Three](#)



81

Day Two

Hoping to be able to better handle the next crisis (this is called *Choose Your Own Disaster* after all) you decide to utilize the team to refine some of your processes and put some improvements into place with tooling that has proven insufficient recently.

This is difficult to do with your limited manpower and doesn't do anything to help your schedule issues, which makes Tina unhappy and doesn't really improve the staff's morale. She hopes that these improvements are worth the additional effort and focus they are getting...

[Proceed to Day Three](#)



82

Day Two

Hoping to be able to better handle the next crisis (this is called *Choose Your Own Disaster* after all) you decide to utilize the team to refine some of your processes and put some improvements into place with tooling that has proven insufficient recently.

This is difficult to do with your limited manpower and doesn't do anything to help your schedule issues, compounding the tasks that have been pushed off to the upcoming sprints. The team is paying the price trying to get caught up and Tina is not happy. She hopes that these improvements are worth the additional effort and focus they are getting...

[Proceed to Day Three](#)



83

Day Two

Hoping to be able to better handle the next crisis (this is called *Choose Your Own Disaster* after all) you decide to utilize the team to create some processes to try and address the situations the company is experiencing.

This is difficult to do with your limited manpower and doesn't do anything to help your schedule issues, which makes Tina unhappy. She hopes that these improvements are worth the additional effort and focus they are getting...

[Proceed to Day Three](#)



84

Day Two

Hoping to be able to better handle the next crisis (this is called *Choose Your Own Disaster* after all) you decide to utilize the team to create some processes to try and address the situations the company is experiencing.

This is difficult to do with your limited manpower and doesn't do anything to help your schedule issues, which makes Tina unhappy and doesn't really improve the staff's morale.

She hopes that these improvements are worth the additional effort and focus they are getting...

[Proceed to Day Three](#)



85

Day Two

Hoping to be able to better handle the next crisis (this is called *Choose Your Own Disaster* after all) you decide to utilize the team to create some processes to try and address the situations the company is experiencing.

This is difficult to do with your limited manpower and doesn't do anything to help your schedule issues, compounding the tasks that have been pushed off to the upcoming sprints. The team is paying the price trying to get caught up and Tina is not happy. She hopes that these improvements are worth the additional effort and focus they are getting...

[Proceed to Day Three](#)

To Infinity And Beyond!
What Could Possibly Go Wrong?

GÜBER

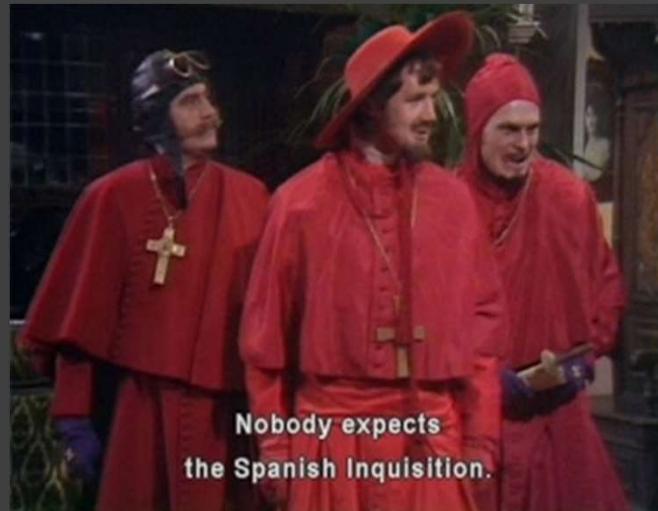
GET A RIDE, ON COMMAND

*Without the annoying driver with
the dubious background!*



MIT grads Shridar Patel, Kurt Wheeling, and Chun Cui have leveraged their fear of interacting with real people and combined that with their passion for building fighting robots.

Again, innately fearing people, the trio have hired a large team of engineers and “product people” to power their vision.



The Corporate Audit team is DELIGHTED you stopped by. They'd LOVE to assist you.



87

“Great! You see someone has posted Randy Quaid’s personal data on the internet....”



[Go to Page 88](#)

“Um....yeah. I’ve got some questions, purely hypothetical, for a friend, you know?”

[Go to Page 64](#)



Back away slowly

[Go to back to Page 157](#)



88



"Oh please, go on..."



"Yeah! So he JUST checked in, so it has to be someone or something that accessed and told the press."

[Go to Page 89](#)



↳

Back away slowly

[Go to back to Page 157](#)





"And when exactly did YOU know about this breach of confidence? What were you doing, precisely, at the time the data was lost?"

Your day ends poorly.

89

Proceed to [Day Three](#)



87

Thoughts of caffeine-fueled work ahead of you puts a smile on your face. You're sure that your SOC employees will operate much more efficiently.



Proceed to [Day Two](#)



08

CBO Fran Cupwell is VERY appreciative for the assistance (her staff got called away to assist in a cleanup in the ER). She opens up a batch of new beans from Kerblackistan called PSYCHOROAST!! ™ and brews you up some liquid gold.

While you are enjoying your hot beverage you read through the instruction manual about how this thing connects to the internet.

Cool, thanks for the cup-a-joe! Talk to you later!

Huh, this is interesting. Ask some more questions



[Go to Day Two](#)



[Go to Page 11](#)



11



The Security Team starts to inquire why a coffee machine needs to be connected to the network

COB Fran Cupwell explains

- that this machine can allow a thirsty patron to order their specialty drink in advance via a mobile app.
- It also sends supply levels to her CCC (Coffee Command Center) so she can reorder beans and filters.
- It also enabled the vendor to do remote maintenance and get diagnostic data to support their maintenance contract

Ask to do an audit of the app & review product deployment documentation

HOLD YOUR HORSES! YOU'RE NOT INSTALLING THIS!



Oh, OK



[Go to Page 12](#)

[Go to Page 91](#)



[Go to Page 36](#)





12

Well that all sounds very nice, super-convenient and customer-focused! The team is really looking forward to having these things online



Proceed to [Day Two](#)

94



Coffee is one of the CORE tenants of the business. The Business reacts poorly to your decision.

Great job! Very impressive! You have a bright future ahead of you as you start your first day of a new job search after you're walked out of the building. Go back to [Page 07](#) and start over.





91

The team does a review and finds the following things:

bla
bla
bla

CBO Fran Cupwell says “Thanks, I didn’t realize all of that. What can we do to fix these things?”

Proceed to [Day Two](#)

Product Reviews





96

Day One

CBO Fran Cupwell completed the Procurement 3rd Party Assessment Form 6 weeks ago. Hasn't anyone from Security gotten to it yet?



Yes, yes. That's in our queue. Bert will be starting that review in maybe 2 weeks.

Uh....We've been ...busy? (scramble to get this done sooner)

HOLD YOUR HORSES! YOU'RE NOT INSTALLING THIS UNTIL WE REVIEW IT!!



[Go to Page 1097](#)



[Go to Page 2098](#)



[Go to Page 94](#)



1097

CBO Fran Cupwell is displeased
with your answer. She will
remember this.



Proceed to [Day Two](#)

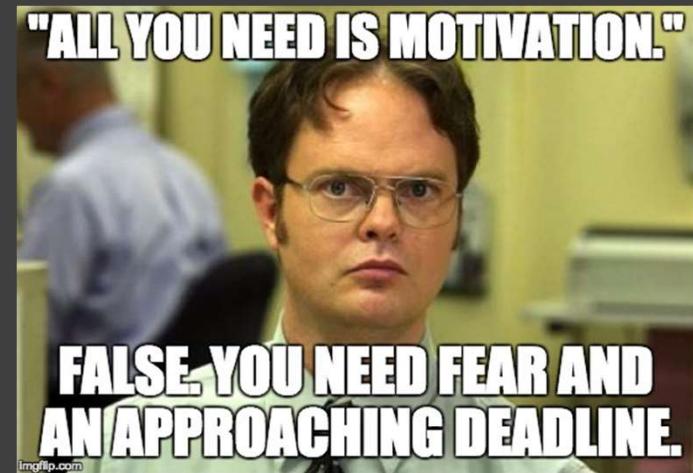


2098

CBO Fran Cupwell thanks you for moving her request up in the queue so these machines can get online quickly (The Stock Brokers from the Wealth Management team are slowing down and need to pick up their pace).

Your “best man” quickly stops what they are doing and rushes through the assessment.

Proceed to [Day Two](#)





Your SOC team comes up to, out of breath from running to find you. An anomalous device has been added to the network and seems vulnerable to EVERY CVE EVER.



79

Day One

Hmm...that sounds bad. We should shut that device off.

Where is the device? Let's play go see.

You're pretty sure whatever it is it can't be THAT bad. You're sure it will fix itself





44

Day One

Anything that bad HAS TO be made up.
You'll have to follow-up with the crew in
the breakroom to see who is goofing on
you.

You're confident this won't still be a
problem tomorrow.



Proceed to [Day Two](#)

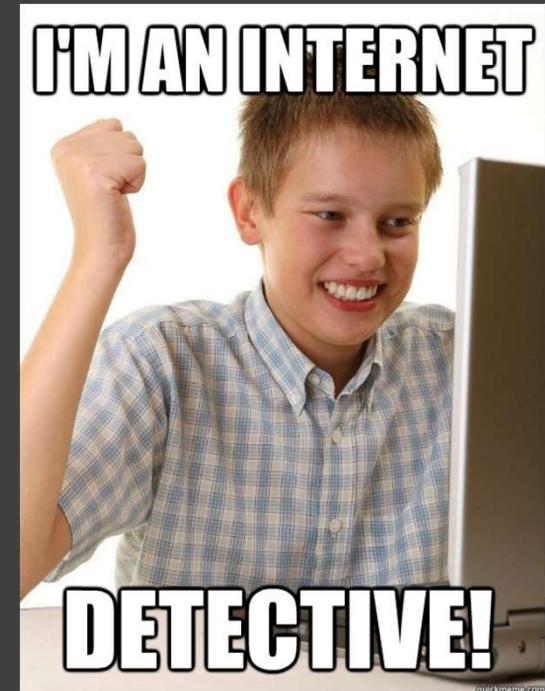


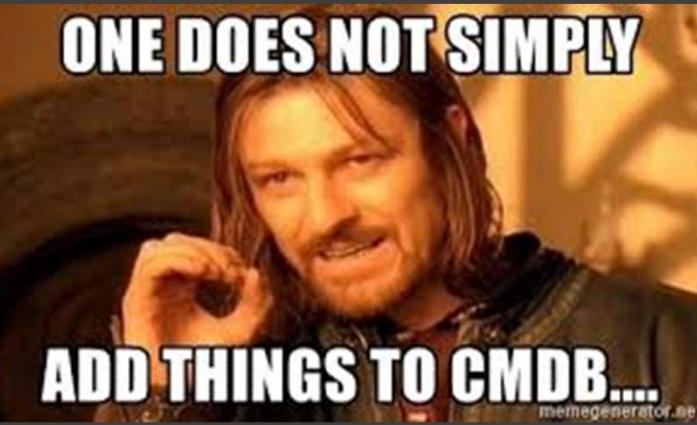
79

Day One

Using the power of HAXORY and half a day's effort you're able to determine that the problem in question is the new network-enabled espresso machines. You've raised some eyebrows, but you think you've covered for initial fire-drill, you hope.

Proceed to [Day Two](#)





ONE DOES NOT SIMPLY

ADD THINGS TO CMDB....

memegenerator.net

Hank McKraken ITILv3, CISA, CSM, PQD, GISS, GOOB, Manager of the Configuration Management Database (CMDB) demands that action be taken! When the grinder came online the CMDB auto-imported invalid data about it and has corrupted all the inputs for today. He demands that **SOMEONE MUST PAY!**

Hmm...that sounds bad. Rules are there for a reason, right? You'll come down **hard** on this infraction.

You'll talk to the CBO and help educate her on the policy for adding devices.



Go to [Page 47](#)



Go to [Page 480](#)



145

Day One



79

Day One

Calling CBO Fran Cupwell into “the big conference room” you and Hank McKraken ITILv3, CISA, CSM, PQD, GISS, GOOB, Manager of the Configuration Management Database lay into her about the multiple violations of policy that transpired.

You block her project for now. Fran Cupwell glares at you across the “big table”. You are sure she will remember this.



Proceed to [Day Two](#)



480

Day One

Taking a more customer-focused tack, you track Fran Cupwell, CBO, down and enjoy a yummy glass of Jamba Juice. You explain the situation, how the CMBD lost days worth of work, and about the risks doing what she just did could incur.

"I never realized everything that goes on 'behind the scenes' here. I'm very sorry, what can I do to do better next time?" Smiling, you both review her current and upcoming projects.

Proceed to [Day Two](#)





Fran Cupwell, Chief Barista Officer, rushes over to you. Her new espresso machines are not functioning. They were plugged in and on for a short while, but suddenly everything stopped. It's CRITICAL that the machines are online and working, a VERY important patient, Randy Quaid, is coming in for a "sensitive procedure" and he and his entourage are espresso-enthusiasts.



Let's go talk to the Network Team

Oh, I know what this is.

If those machines aren't working they'll probably give Hospital Bank & Roastery (est. 2018) bad Yelp! reviews



Go to [Page 50](#)



Go to [Page 254](#)



246

Day One

246

Day One



You journey down into the bowels of the Hospital Bank & Roastery (est 2018) headquarters.... into.... **the IT department.**

You talk to Rory Thistlebrush, head of Networking. He looks at you in horror. A *Business Person*.....here....gasp!

He listens intently as Fran Cupwell describes the problem. He even grins a little at one point. “Yes. That sounds like you’ve fallen into my beautifully designed Network Authentication program (mwahahaha.)

So....is there anything we can do about that?

Help articulate Fran’s case



[Go to Page 51,002](#)



[Go to Page 53](#)





246

Day One

“Of course there is NOTHING you can do
(mwahaha.).”

Fran has a white-knuckled grip on her little espresso cup, her eyebrows furrowing.



“Well, that sure sounds pretty final.”



Go to [Page 52](#)

“So....is there anything we can do about that?”

Go to [Page 53](#)





52

Day One

CBO Fran Cupwell is displeased with your answer. She will remember this.



Proceed to [Day Two](#)

246

Day One



“Award-winning ACTOR Randy Quaid?
HERE?!? At the Hospital Bank and Roastery
(est 2018)? Egads! That certainly sounds
important for our company!”

He ponders for a moment.

“Perhaps we can fill out the necessary forms
right now and I'll have Janelle, my lead
firewall engineer, open things up
immediately!”



Proceed to [Day Two](#)



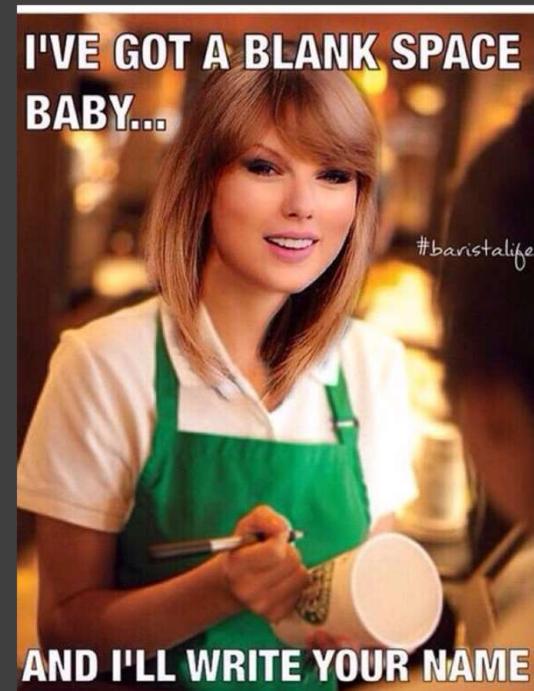
254

Day One

Taking a more customer-focused tack, you track Fran Cupwell, CBO, down and enjoy a yummy glass of Jamba Juice. You explain the situation, how and why devices get added to the network, and about the risks doing what she just did could incur.

"I never realized everything that goes on 'behind the scenes' here. I'm very sorry, what can I do to do better next time?" Smiling, you both review her current and upcoming projects.

Proceed to [Day Two](#)





111

Day Two

You journey down into the bowels of the Hospital Bank & Roastery (est 2018) headquarters.... into.... **the IT department.**

You talk to Rory Thistlebrush, head of Networking. He looks at you in horror. A *Business Person*.....here....gasp!

He listens for a bit then starts complaining that he doesn't have time to deal with this and you should put a service request in and his team will respond to you within the documented SLA. You try to rebut, but he wishes you "Good Day Sir. No! I said GOOD DAY!"

That's not the news you were hoping for.



Proceed to [Day Three](#)



42

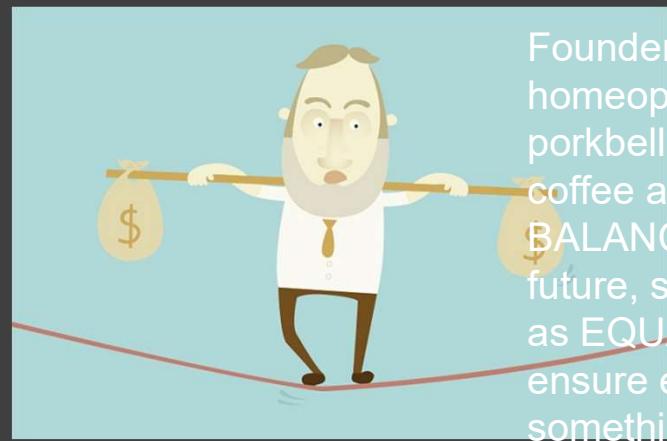
Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that a **BALANCED APPROACH** is the future, so he **SPLITS** his funding as **EQUALLY** as possible to ensure everyone gets a little something.

42

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that a **BALANCED APPROACH** is the future, so he **SPLITS** his funding as **EQUALLY** as possible to ensure everyone gets a little something.



In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 225](#)

[Go to Page 213](#)





In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 225](#)



[Go to Page 214](#)



[Go to Page 227](#)

115

Day Three



In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 225](#)



[Go to Page 215](#)



[Go to Page 226](#)

116

Day Three



In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 225](#)



[Go to Page 216](#)



[Go to Page 227](#)

117

Day Three



118

Day Three



In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 228](#)



[Go to Page 217](#)



[Go to Page 229](#)



119

Day Three



In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 228](#)

[Go to Page 218](#)



[Go to Page 230](#)





In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 228](#)



[Go to Page 219](#)



[Go to Page 229](#)

120

Day Three



In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 228](#)

[Go to Page 220](#)





In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 231](#)



[Go to Page 221](#)



[Go to Page 232](#)

122

Day Three



In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 231](#)



[Go to Page 222](#)



[Go to Page 233](#)

123

Day Three



In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 231](#)

[Go to Page 223](#)





In your e-mail the next morning you see a message from a reporter about a vulnerability that could possibly affect a minor component in your SpiffyCloud application. Supposedly this flaw could enable an attacker to remotely execute code on the server.

There is a lot of other stuff on your plate right now though and Tina's patience seems to be running quite thin...

What do you do?

Meh, we have more important stuff to worry about than a *possible* vulnerability.

ZOMG! Pull everyone in and check every line of code!

Let's get a small group to analyze the flaw and see if we are affected.



[Go to Page 231](#)



[Go to Page 224](#)



[Go to Page 233](#)

125

Day Three

I iz in yur computer



stealing yur dataz

Text

What do you do?



XX

Day Three

Option 1



Go to Page xx

Option 2



Go to Page xx

Option 3



Go to Page xx



Founder Dr. Churles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PROCESS is the key, so overwhelming funds finding the best and brightest checklists and processes his espresso-stain dollars can buy.



362

Day One



Founder Dr. Churles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PROCESS is the key, so overwhelming funds finding the best and brightest checklists and processes his espresso-stain dollars can buy.



362

Day One



Founder Dr. Churles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PROCESS is the key, so overwhelming funds finding the best and brightest checklists and processes his espresso-stain dollars can buy.



362

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that TECHNOLOGY is the future, so overwhelming funds finding the best and brightest TOOLS his espresso-stain dollars can buy.



79

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that TECHNOLOGY is the future, so overwhelming funds finding the best and brightest TOOLS his espresso-stain dollars can buy.



79

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that TECHNOLOGY is the future, so overwhelming funds finding the best and brightest TOOLS his espresso-stain dollars can buy.



0

79

Day One

42

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that a **BALANCED APPROACH** is the future, so he **SPLITS** his funding as **EQUALLY** as possible to ensure everyone gets a little something.

42

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that a **BALANCED APPROACH** is the future, so he **SPLITS** his funding as **EQUALLY** as possible to ensure everyone gets a little something.



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that a **BALANCED APPROACH** is the future, so he **SPLITS** his funding as **EQUALLY** as possible to ensure everyone gets a little something.



42

Day One

Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PEOPLE are the future, so overwhelming funds finding the best and brightest people his espresso-stain dollars can buy.

Day One

Race around in a panic!



[Go to Page 200](#)

Call Physical Security!



[Go to Page 98](#)

In wait, we moved all our servers to the cloud last week



[Go to Page 25](#)

Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PEOPLE are the future, so overwhelming funds finding the best and brightest people his espresso-stain dollars can buy.

Day One

Race around in a panic!



[Go to Page 200](#)

Call Physical Security!



[Go to Page 98](#)

In wait, we moved all our servers to the cloud last week



[Go to Page 25](#)

Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PEOPLE are the future, so overwhelming funds finding the best and brightest people his espresso-stain dollars can buy.

Day One

Race around in a panic!



[Go to Page 200](#)

Call Physical Security!

[Go to Page 98](#)



In wait, we moved all our servers to the cloud last week

[Go to Page 25](#)



362

Day One



Founder Dr. Churles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PROCESS is the key, so overwhelming funds finding the best and brightest checklists and processes his espresso-stain dollars can buy.

Founder Dr. Churles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PROCESS is the key, so overwhelming funds finding the best and brightest checklists and processes his espresso-stain dollars can buy.

362

Day One

362

Day One

Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that PROCESS is the key, so overwhelming funds finding the best and brightest checklists and processes his espresso-stain dollars can buy.





Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that TECHNOLOGY is the future, so overwhelming funds finding the best and brightest TOOLS his espresso-stain dollars can buy.

79

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that TECHNOLOGY is the future, so overwhelming funds finding the best and brightest TOOLS his espresso-stain dollars can buy.

79

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that TECHNOLOGY is the future, so overwhelming funds finding the best and brightest TOOLS his espresso-stain dollars can buy.

79

Day One

42

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that a **BALANCED APPROACH** is the future, so he **SPLITS** his funding as **EQUALLY** as possible to ensure everyone gets a little something.

42

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that a **BALANCED APPROACH** is the future, so he **SPLITS** his funding as **EQUALLY** as possible to ensure everyone gets a little something.

42

Day One



Founder Dr. Charles Manbun III, a homeopathic brain surgeon, porkbelly futures maven, and coffee aficionado thinks that a BALANCED APPROACH is the future, so he SPLITS his funding as EQUALLY as possible to ensure everyone gets a little something.

01



Day One

02



Day Two

03



Day Three



CEO and Chairman of the Board, Dr. Charles Manbun III, a homeopathic vegan brain surgeon, porkbelly futures maven, and coffee aficionado receives a phonecall. Hospital Bank & Roastery (est 2018) will be having a very prestigious patient this week: The award-winning star of stage and screen, Randy Quaid, will be coming in for a “sensitive procedure”



Sounds GREAT! Randy Quaid is a man of the people, like Cousin Eddie from the National Lampoons Vacation Saga, and we funded our security budget focused on PEOPLE!



[Go to Page 87](#)



02

Day Two



Hours later you get a call from your corporate counselor, Bob Loblaw. He was updating his Law Blog and saw these STUNNING headlines!



He needs you to get to the root of the matter ASAP! Someone is leaking confidential patient data!

Golly! You're SURE that's not as bad as it looks!

Let's roll out the security dragnet and see what our experts come up with

But wait... we've provided HIPAA compliance training!



[Go to Page 95](#)

[Go to Page 960](#)



[Go to Page 09](#)



87

Day Two

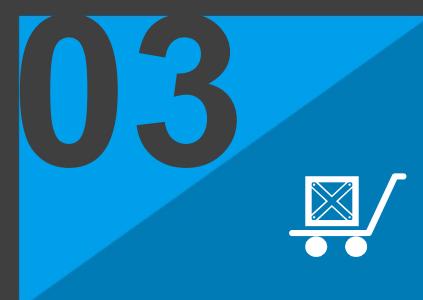




Day One



Day Two



Day Three



CEO and Chairman of the Board, Dr. Charles Manbun III, a homeopathic vegan brain surgeon, porkbelly futures maven, and coffee aficionado receives a phonecall. Hospital Bank & Roastery (est 2018) will be having a very prestigious patient this week: The award-winning star of stage and screen, Randy Quaid, will be coming in for a “sensitive procedure”



Sounds GREAT! Randy Quaid is a man of the people, like Cousin Eddie from the National Lampoons Vacation Saga, and we funded our security budget focused on PEOPLE!

It's a good thing we funded our TECHNOLOGY, Randy Quaid used that to stop the aliens in ID4!



[Go to Page 87](#)

[Go to Page 11](#)



02

Day Two



Hours later you get a call from your corporate counselor, Bob Loblaw. He was updating his Law Blog and saw these STUNNING headlines!



He needs you to get to the root of the matter ASAP! Someone is leaking confidential patient data!

Golly! You're SURE that's not as bad as it looks!

Let's roll out the security dragnet and see what our experts come up with

But wait... we've provided HIPAA compliance training!



[Go to Page 87](#)

[Go to Page 08](#)



[Go to Page 11](#)



02

Day Two





Hours later you get a call from your corporate counselor, Bob Loblaw. He was updating his Law Blog and saw these STUNNING headlines!



He needs you to get to the root of the matter ASAP! Someone is leaking confidential patient data!

Golly! You're SURE that's not as bad as it looks!

Let's go check our awesome data googleplexer-detector-thingy that goes "Bing"

But wait... we've provided HIPAA compliance training!



[Go to Page 87](#)

[Go to Page 08](#)



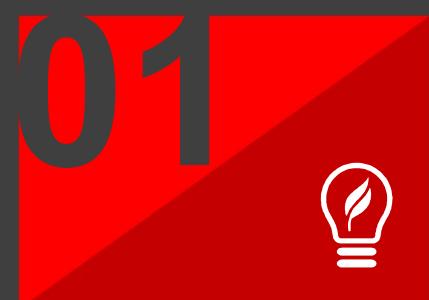
[Go to Page 11](#)



02

Day Two

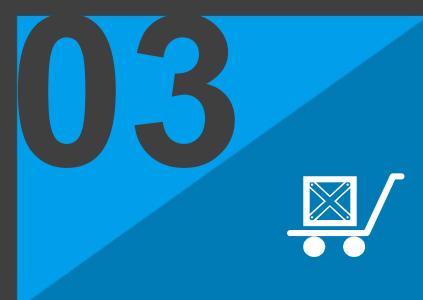




Day One



Day Two



Day Three



CEO and Chairman of the Board, Dr. Charles Manbun III, a homeopathic vegan brain surgeon, porkbelly futures maven, and coffee aficionado receives a phonecall. Hospital Bank & Roastery (est 2018) will be having a very prestigious patient this week: The award-winning star of stage and screen, Randy Quaid, will be coming in for a “sensitive procedure”



It's great that we funded our PROCESSES. We hear that Randy Quaid is a method actor and is ALL about process!

It's a good thing we funded our TECHNOLOGY, Randy Quaid used that to stop the aliens in ID4!

[Go to Page 157](#)



[Go to Page 11](#)



02

Day Two





Hours later you get a call from your corporate counselor, Bob Loblaw. He was updating his Law Blog and saw these STUNNING headlines!



He needs you to get to the root of the matter ASAP! Someone is leaking confidential patient data!

Well let's pull out our playbook for what to do with this type of event.

Let's go check our awesome data googleplexer-detector-thingy that goes "Bing"

Hmm.... let's go check with Corporate Compliance, obviously someone didn't follow the process



[Go to Page 208](#)

[Go to Page 159](#)



[Go to Page 87](#)



157

Day Two





Hours later you get a call from your corporate counselor, Bob Loblaw. He was updating his Law Blog and saw these STUNNING headlines!



He needs you to get to the root of the matter ASAP! Someone is leaking confidential patient data!

Quick! Let's go look in the SIEM!

Let's go check our awesome data googleplexer-detector-thingy that goes "Bing"

Can't the Network team figure this out?



[Go to Page 206](#)

[Go to Page 159](#)



[Go to Page 190](#)



02

Day Two





159

Day Two

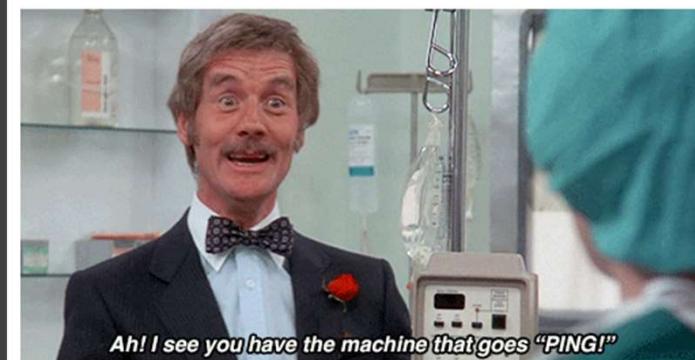
You're sure glad that you spent all your budget on this fancy thing. You're not sure everything it does, but it sure as heck looks impressive doing it!

The machine churns away for awhile and spits out some data.

Great! Rush this info straight to the CTO!

With your mom being Sarah Connor, you inherently don't trust machines. Give the data a quick review

Consult with some of your peers



Ah! I see you have the machine that goes "PING!"



[Go to Page 95](#)



[Go to Page 08](#)



[Go to Page 11](#)



You rush to CTO Bjorn Borgenson's well-lit corner office, a trail of greenbar paper from the Machine that goes 'Bing' streaming behind you. You slam it down on his desk. "Ah-HA! This printout tells us EXACTLY who leaked Randy Quaid's information!"

He stares at you blankly, the scrawl of numbers and letters not meaning anything to you. After a long period of silence he hand you an empty box and suggests you might benefit from packing up your desk into it.

Maybe you'll do better the next place you work.
Too bad about Randy's data. Go back to [Page 151](#) and start over.



Hours later you get a call from your corporate counselor, Bob Loblaw. He was updating his Law Blog and saw these STUNNING headlines!



02

Day Two

Sounds GREAT! We LOVE the smell of freshly ground beans in the morning

Who doesn't love a good coffee? Offer to help her unbox and setup the new machines

Wait. Network wut?



[Go to Page 87](#)

[Go to Page 08](#)





95

The CEO asks you into his office to play a short game on his whiteboard. You're neither good at protecting sensitive data nor hangman.

Maybe you'll do better the next place you work.
Too bad about Randy's data. Go back to [Page 140](#) and start over.





960

Day Two

You get Scoob and the Gang together to start sifting through what little data you have. You don't have a lot of time to get back to Legal. Where do you start your investigation?



Who has access to Randy Quaid's data?



[Go to Page 95](#)

What systems does Randy Quaid's data live in?



[Go to Page 08](#)

All this thinking makes you thirsty. Decide to head down to the Cantina for a tasty coffee!



[Go to Page 11](#)



What systems contain patient data? Sure is a good thing Ian the IT guy wrote that down in a Visio diagram somewhere. Now....where was that saved? Unfortunately Ian is on PTO today.

02

Day Two

Ian keeps everything on the IT wiki.



[Go to Page 95](#)

Ian told Andy who surely told Rachel. Go ask her.

[Go to Page 08](#)



Google around the corporate intranet.

[Go to Page 11](#)





You talk to Nurse J, head of Nursing. She's taken aback at the implication that ANYONE at Hospital Bank & Roastery (est 2018) would POSSIBLY do such a thing!

She gets you a list of people that have access to the systems that hold patient data. What do you do with it?

02

Day Two

All kids like LOG! Dive into the access logs and find out who touched Randy's records!

Let's roll out the security dragnet and see what our experts come up with

But wait... we've provided HIPAA compliance training!



[Go to Page 95](#)



[Go to Page 08](#)



[Go to Page 11](#)



ONE SIMPLY DOES NOT

WORK WITHOUT COFFEE.

makeameme.org

A nice hot coffee will clear your head.



02

Day Two

Look around the cantina, see what's new.



[Go to Page 95](#)



[Go to Page 08](#)



[Go to Page 11](#)

Enjoy that hot cup-a-joe and kick back, try to forget about your stressful day

Ok, that's a long enough break! You have Randy Quaid's data to protect!



02

Day Two

Wiki-wiki-wiki! You boot up the intranets and log into the IT Wiki site.

THERE'S A WIKI FOR THAT?

NO WAY!

Well here's a diagram. It's a year old, but that's probably good enough

Ew. This diagram is super-old. You probably should call Ian. He's on his honeymoon, but this is important, you're sure he won't mind.



[Go to Page 95](#)

[Go to Page 08](#)





02

Day Two

You catch up with Rachel and ask her about Ian's documentation. She's pretty sure Ian hadn't drawn the network diagram yet. He DID have a sketch of it in his "work notes" notebook. That ratty old thing normally sits on his desk.



Go check out Ian's desk



[Go to Page 159](#)

Man. This is a lot of work. You're sure someone else is searching too. Go take a break.

[Go to Page 11163](#)





95

Speaking of hassles...it sure is a drag when you have to cram all your stuff into a box after they let you go for negligence.

You also not only have made Randy Quaid cry, but you've inspired him to sue your company out of existence.

Maybe you'll do better the next place you work. Too bad about Randy's data. Go back to [Page 140](#) and start over.





Well, the office pranksters have been at Ian's desk. You spend a few minutes looking over his stuff for the notebook. You find the list of all server IPs. You get the termination report for tomorrow (sorry to hear Rachel won't be around tomorrow afternoon)



170

Day Two

Oh well. You're sure this can wait until Ian gets back.

ZOMG! Shenanigans are afoot! Call Physical Security!



[Go to Page 95](#)



[Go to Page 160](#)



160

Day Two

Your partners in physical security immediately leap to action.



"You know, I was watching this shady character wearing a contractor badge skulking around this area. I think I saw him to to the underbasement!"



[Go to Page 159](#)

"Thank you for the report. We'll keep and eye out for any suspicious activity. Think you could get Randy Quaid to autograph this?"

[Go to Page 162](#)





95

Going to the underbasement was a poor choice.

Your legend will live on in tales around the water cooler for days to come.

Go back to [Page 140](#) and start over.

IT IS PITCH BLACK.



YOU ARE LIKELY TO BE EATEN
BY A GRUE.



Uh.... I guess so.



159

Day Two

You guess it wouldn't be a big hassle. Randy Quaid probably wouldn't mind signing something for a super-fan.



[Go to Page 158](#)

No. Wait. Seriously. He needs to write this up.

[Go to Page 163](#)





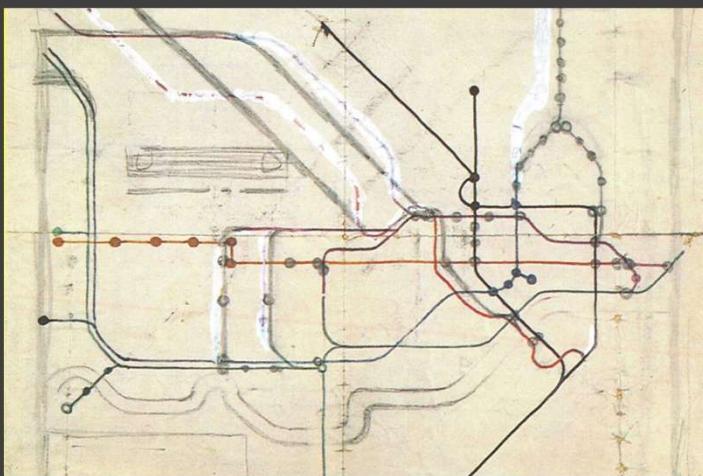
163

Day Two

Physical Security is displeased with your answer. They will remember this.



Proceed to [Day Three](#)



Wow. This thing looks like it was written on parchment paper, scanned, then faxed in and uploaded to the Wiki.



159

Day Two

Good enough. Pass this over to Operations to decipher.



[Go to Page 158](#)



[Go to Page 163](#)

Maybe you should spend some time looking more into this and how all this plugs together.



165

Day Two



You call Ian on his tropical honeymoon. His bride Shelly is displeased. Ian tries to be helpful, but the resort limbo competition is about ready to start. He feels that he and Shelly have a good chance to get a medal.

By the end of the day you only have a server name that has open firewall ports to the patient database: "CFFEGRNDR01"
...whatever the heck THAT is. Oh well, this will probably all take care of itself tomorrow.

Proceed to [Day Three](#)

163

Day Two

Yeah, those guys down in Ops should be able to figure things out. You throw this problem over the wall and go to lunch.



Proceed to [Day Three](#)



163

Day Two

Management is bringing pizza in for lunch today, so you have some time.

How would you understand what systems have access to patient data using this diagram?



You've heard of this awesome tool called WireBearSnort. Maybe download that and try it out?

Take the diagram to the Network team.



[Go to Page 158](#)

[Go to Page 163](#)





DHQteam/tremantw

The most interesting and useful things can be found on the internet! You download your copy of WireBearSnort and after a few quick clicks and some annoying permission requests you're up and WireBearing away!

4 3.0155090000	74.125.68.94	192.168.0.6	TCP	66 443-51660 [ACK] Seq=1 Ack=155 Win=391 Len=0 Tsval=2954786
5 3.0321090000	74.125.68.94	192.168.0.6	TLSv1.2	163 Application Data
6 3.0321030000	74.125.68.94	192.168.0.6	TLSv1.2	183 Application Data
7 3.0322570000	192.168.0.6	74.125.68.94	TCP	66 51660-443 [ACK] Seq=155 Ack=98 Win=8185 Len=0 Tsval=71212
8 3.0322580000	192.168.0.6	74.125.68.94	TCP	66 51660-443 [ACK] Seq=155 Ack=215 Win=8178 Len=0 Tsval=71212
9 3.0328440000	74.125.68.94	192.168.0.6	TLSv1.2	112 Application Data
10 3.0328960000	192.168.0.6	74.125.68.94	TCP	66 51660-443 [ACK] Seq=155 Ack=261 Win=8189 Len=0 Tsval=71212
11 3.0329910000	192.168.0.6	74.125.68.94	TLSv1.2	112 Application Data
12 3.1887120000	74.125.68.94	192.168.0.6	TCP	66 443-51660 [ACK] Seq=261 Ack=201 Win=391 Len=0 Tsval=2954786
16 6.1407900000	192.168.0.6	74.125.68.94	TLSv1.2	220 Application Data
22 6.2403350000	74.125.68.94	192.168.0.6	TCP	66 443-51660 [ACK] Seq=261 Ack=355 Win=405 Len=0 Tsval=2954786
23 6.2792630000	74.125.68.94	192.168.0.6	TLSv1.2	163 Application Data
24 6.2793220000	192.168.0.6	74.125.68.94	TCP	66 51660-443 [ACK] Seq=355 Ack=358 Win=8185 Len=0 Tsval=71212
25 6.2814370000	74.125.68.94	192.168.0.6	TLSv1.2	385 Application Data
26 6.2814420000	74.125.68.94	192.168.0.6	TLSv1.2	112 Application Data
27 6.2815740000	192.168.0.6	74.125.68.94	TCP	66 51660-443 [ACK] Seq=355 Ack=677 Win=8172 Len=0 Tsval=71212
28 6.2815750000	192.168.0.6	74.125.68.94	TCP	66 51660-443 [ACK] Seq=355 Ack=723 Win=8169 Len=0 Tsval=71212
29 6.2820170000	192.168.0.6	74.125.68.94	TLSv1.2	112 Application Data
37 6.4422430000	74.125.68.94	192.168.0.6	TCP	66 443-51660 [ACK] Seq=723 Ack=401 Win=405 Len=0 Tsval=2954786
41 6.6383660000	192.168.0.6	74.125.68.94	TLSv1.2	178 Application Data
42 6.7525190000	74.125.68.94	192.168.0.6	TCP	66 443-51660 [ACK] Seq=723 Ack=513 Win=405 Len=0 Tsval=2954786
43 6.8180560000	74.125.68.94	192.168.0.6	TLSv1.2	151 Application Data
44 6.8182150000	74.125.68.94	192.168.0.6	TLSv1.2	1484 Application Data
45 6.8182360000	192.168.0.6	74.125.68.94	TCP	66 51660-443 [ACK] Seq=513 Ack=808 Win=8186 Len=0 Tsval=71212
46 6.8182970000	192.168.0.6	74.125.68.94	TCP	66 51660-443 [ACK] Seq=513 Ack=2226 Win=8103 Len=0 Tsval=71212
47 6.8189200000	74.125.68.94	192.168.0.6	TLSv1.2	1484 Application Data

Sadly, the output is a bit cryptic....

Hold my beer! You've got this!



[Go to Page 158](#)

Maybe those guys in Ops should handle this?

[Go to Page 163](#)



159

Day Two





163

Day Two

That which does not kill you makes you stronger.
You read that once somewhere.

You spend the rest of the day googling around and reading tutorials and finally discover that the only system that could access the patient database server is something called “CFFEGRNDR01”. It was just added to the network yesterday and started connecting to any open services on the network.

That's pretty weird.

Proceed to [Day Three](#)



02

Day Two



You open the access logs.....

```
1 [k daemon not running, starting it now on port 5037 *
2 * daemon started successfully *
3 ----- beginning of system
4 D/ActivityManager( 801): retrieveServiceLocked(): component = com.google.android.gms/com.google.android.gms
5 D/ActivityManager( 801): caller:android.app.ApplicationThreadProxy@3211d60, r.packageName :com.google.android.gms
6 D/ActivityManager( 801): startService callerProcessName:com.google.android.gms, calleePkgName: com.google.android.gms
7 D/ActivityManager( 801): retrieveServiceLocked(): component = com.google.android.gms/com.google.android.gms
8 D/ActivityManager( 801): caller:android.app.ApplicationThreadProxy@1edce2de, r.packageName :com.google.android.gms
9 D/ActivityManager( 801): startService callerProcessName:com.google.android.googlequicksearchbox, calleePkgName: com.google.android.googlequicksearchbox
10 D/ActivityManager( 801): retrieveServiceLocked(): component = com.google.android.googlequicksearchbox/com.google.android.googlequicksearchbox
11 D/ActivityManager( 801): caller:android.app.ApplicationThreadProxy@363196d5, r.packageName :com.google.android.googlequicksearchbox
12 D/ActivityManager( 801): startService callerProcessName:com.google.android.gms, calleePkgName: com.google.android.gms
13 D/ActivityManager( 801): retrieveServiceLocked(): component = com.google.android.gms/com.google.android.gms
14 D/ActivityManager( 801): caller:android.app.ApplicationThreadProxy@8d93878, r.packageName :com.google.android.gms
15 D/ActivityManager( 801): retrieveServiceLocked(): component = null; callingUser = 0; userId(target) = 0
16 D/ActivityManager( 801): startProcessLocked calleePkgName: com.samsung.klmsagent, hostingType: broadcast
17 W/ActivityThread(10898): ClassLoader.loadClass: The class loader returned by Thread.getContextClassLoader() is null
18 E/ActivityManager( 801): checkUser: useridlist=null, currentuser=0
19 E/ActivityManager( 801): checkUser: useridlist=null, currentuser=0
20 E/ActivityManager( 801): checkUser: useridlist=null, currentuser=0
21 E/ActivityManager( 801): checkUser: useridlist=null, currentuser=0
22 I/libpersona(10972): KNOX_SDCARD checking this for 10012
23 I/libpersona(10972): KNOX_SDCARD not a persona
24 I/ActivityManager( 801): Start proc com.samsung.klmsagent for broadcast com.samsung.klmsagent/.listner.Main
25 I/ActivityManager( 801): Killing 10537:com.sec.android.sidesync30/u0a127 (adj 15): empty #25
```

....uuuhhhh

Roll up your sleeves and figure this out

Man. This seems like a lot of work. Maybe the Ops team can do this?

Turn the list over to Physical Security.
Obviously they are trained to deal with this!





02

Day Two

Your partners in Physical Security seem receptive to your questions.



Yeah, you know we've got a perp we've been keeping an eye on!

What is this log you speak of?

Want for us to ask around?



[Go to Page 95](#)



[Go to Page 08](#)



[Go to Page 11](#)



02

Day Two

After many hours of sifting through the logs you find one strange IP address and user account coming up frequently accessing the patient database.



Ask around for info about that computer & user.

Maybe we should go talk to the Network team?

Turn the list over to Physical Security.
Obviously they are trained to deal with this!



[Go to Page 95](#)



[Go to Page 08](#)

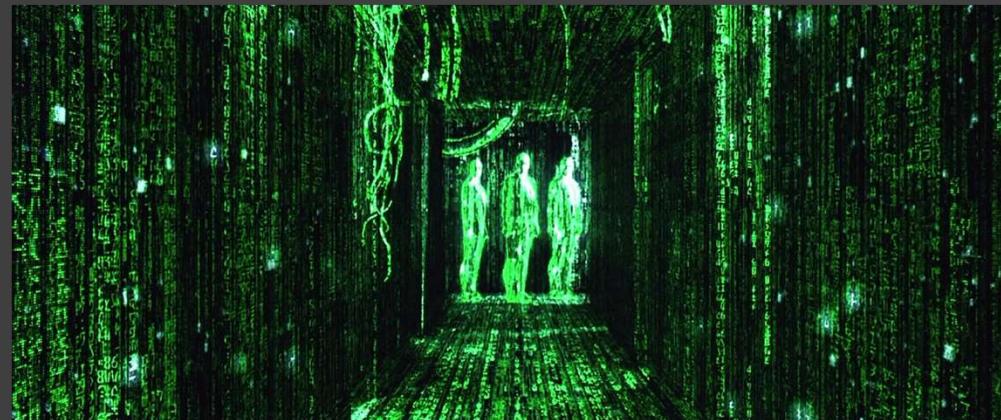


[Go to Page 11](#)



"Oh my stars and garters! What in the wide world of sports is THAT? Is that even a language used to communicate somehow?

Together you and PhysSec spend the afternoon staring at the screen, somehow trying to decipher the matrix.



[Proceed to Day Three](#)



159

Day Two



159

Day Two



You ask around. Paul from Physical Security heard that apparently one of the contractors has been talking about how big a fan of Randy Quaid he is.

Do you want to question the contractor?

Yeah! Obviously this guy is our leaker!

It can't hurt to ask some questions.

You know, this is all probably just a misunderstanding. Let's not act too hastily.





159

Day Two



“Easy there Cowboy!” Paul yells, inserting himself between the contractor and the door as he was leaving for the day. “We have some questions for you!”

“What’s all this suspicious activity in this log thingy coming from your computer?”

“I don’t know what you’re talking about, sir.”



[Go to Page 95](#)

“I didn’t do anything wrong!”



[Go to Page 08](#)



02

Day Two

You explain what you're seeing. The contractor thinks for a bit. "I haven't done anything different today than I do other days." You continue talking, and suddenly they say....

"I did find a thumb drive in the parking lot this morning, but when I plugged it into my workstation nothing happened."



"Could we see that drive please?"



Man! That guy's lucky! Free USB drive. If only you ever had that kind of luck!





You do some analysis on the thumb drive from an isolated workstation. There's a program on it that searches out open network shares and apparently copies the data off the system to some address in the Caymen Islands. That's weird.

159

Day Two

[Proceed to Day Three](#)

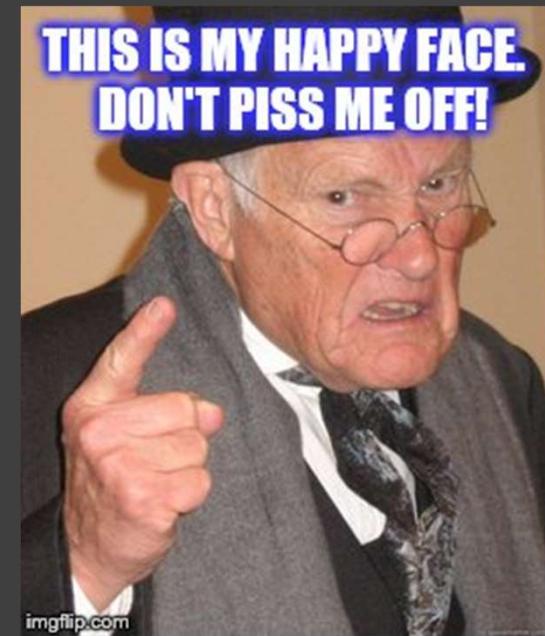


02

Day Two

He gets angry and starts wagging his finger at you. "I don't know why you're harassing me. I didn't do anything wrong and if you bother me again without FACTS I'm calling HR on you."

With that he storms off.



Proceed to [Day Three](#)



190

Day Two

You journey down into the bowels of the Hospital Bank & Roastery (est 2018) headquarters.... into.... **the IT department.**

You talk to Rory Thistlebrush, head of Networking. He looks at you in horror. A *Business Person*.....here....gasp!

He listens intently as you describes the problem. He even grins a little at one point.
“Yes. That sounds like deeply NEED our help (mwahahaha.)”

So....is there anything we can do about that?

Help articulate the impact to the business



[Go to Page 51,002](#)



[Go to Page 53](#)





246

Day One

“Of course there is NOTHING you can do
(mwahaha.).”



“Well, that sure sounds pretty final.”



[Go to Page 52](#)

“So....is there anything we can do about that?”



[Go to Page 53](#)



246

Day One

“Award-winning ACTOR Randy Quaid?
HERE?!? At the Hospital Bank and Roastery
(est 2018)? Egads! That certainly sounds
important for our company!”

He ponders for a moment.

“Perhaps we can assist. I’ll have Janelle, my
lead firewall engineer, sit with you to track
this nefarious traffic down immediately!
(mwa-ha)”



Proceed to [Day Three](#)



246

Day One

Corporate Council Bob Loblaw is displeased
with your lack of action.



Proceed to [Day Three](#)



246

Day One

Oh yeah.... HIPAA training. Everyone always pays attention to the annual compliance tests! Yay team! This one is in the bag!

EVERYDAY IS



@brianlopezit
TRAINING DAY

Proceed to [Day Three](#)

02

Day Two



Wiki-wiki-wiki! You boot up the intranets and log into the IT Wiki site.



Well here's a diagram. It's a year old, but that's probably good enough

Ew. This diagram is super-old. You probably should call Ian. He's on his honeymoon, but this is important, you're sure he won't mind.



[Go to Page 95](#)

[Go to Page 08](#)





02

Day Two

Yeah man, we'll just take a few minutes to search around....



Oh man..... look at all these sick cat memes!
Sweet! I LOVE those!



[Go to Page 95](#)

You poke around a bit more. Maybe you're not using the right search terms

[Go to Page 08](#)



SITS IN

HUMAN

YOUR F

I HAVE TO RU
FAST AS I C

SI

Your face.

JIMEUW

DONT MIND ME

Proceed to [Day Three](#)



246

Day One

The afternoon slips by. The internal search engine can not find the file you're looking for. As the sun sets outside you look up forgetting what it was you intended to do.

Proceed to [Day Three](#)





246

Day One

Interesting. Fran Cupwell, Chief Barista Officer is glowering angrily at her new bank of espresso machines.



That's a shame. I hope her days gets better.
Ah well, back to work!

Ask Fran if she needs any help.



[Go to Page 95](#)



[Go to Page 08](#)



246

Day One

The afternoon slips by. You see the sun slowly set off in the horizon. The fragrant smells of the coffee beans fill your nose as well as your soul.

Uh.....why were you here? Oh well, your spirits uplifted you collect your bag and head home for the night.



Proceed to [Day Three](#)



You talk with Fran, and apparently her new network-enabled espresso machines have been acting weird all day.

"That sure is too bad. I hope you get that figured out!" You go back and enjoy your coffee



Go to [Page 95](#)

"Well, let's see what these little fellas are doing."



Go to [Page 08](#)



159

Day Two



246

Day One

You get your laptop and try to get into the remote console for the unit. The password it should be has been changed and you're locked out. You do some packet capturing and see her coffee machines are spamming the network, trying to connect to fileshares and then to sites outside of your network.

That doesn't sound right. You explain this and unplug them for now. You'll need to get the Network team and Ops teams to help troubleshoot this.

Proceed to [Day Three](#)





02

Day Two

Leaking confidential patient data is bad. You'll drop everything and jump onto this!



The Network team should be able to help us here



[Go to Page 95](#)

You don't need help yet. Heck, you hardly even know what the problem is. Take a minute to think this through

[Go to Page 08](#)

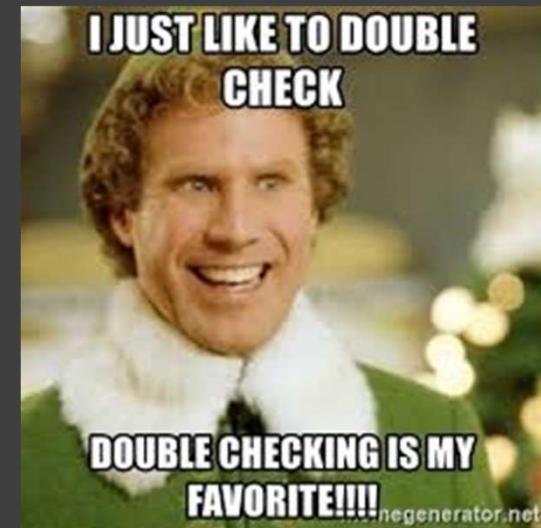




02

Day Two

Hey! Hospital Bank and Roastery (est 2018) has a lot of great people you could consult with!



The Network Team is always...kind ofhelpful



[Go to Page 95](#)

How about Ian in Ops?

[Go to Page 08](#)



I HEARD YOU LIKE OPS

SO WE HAVE AN OPS TEAM FOR
YOUR OPS TEAMS

MemesHappen

Yeah! That Ian, he's a real mensch. Our Ops team is GREAT! You're sure he'll help you out!



Well, you're sure he wouldn't mind *one* little phone call!

No, PTO is PTO. We'd better plan for something else. Back to the drawing board.



Go to [Page 95](#)



Go to [Page 08](#)



159

Day Two



206

Day Two

Oooh Shiny! If it happens, you KNOW your SEIM captures it. Now...where would you find it?



Easy-peasy.... you can figure this out! (gulp!)



[Go to Page 95](#)

Look around for a bit, then ask Nick the SOC manager for help.



[Go to Page 08](#)



Nick looks up at you from his game of Minesweeper like you have 3 heads.

“Can I HELP you with something?”

“Actually yes Nick. I need your help finding some information about a possible data breach.”

“Um, I suppose not. I can figure it out myself.”



Go to [Page 95](#)

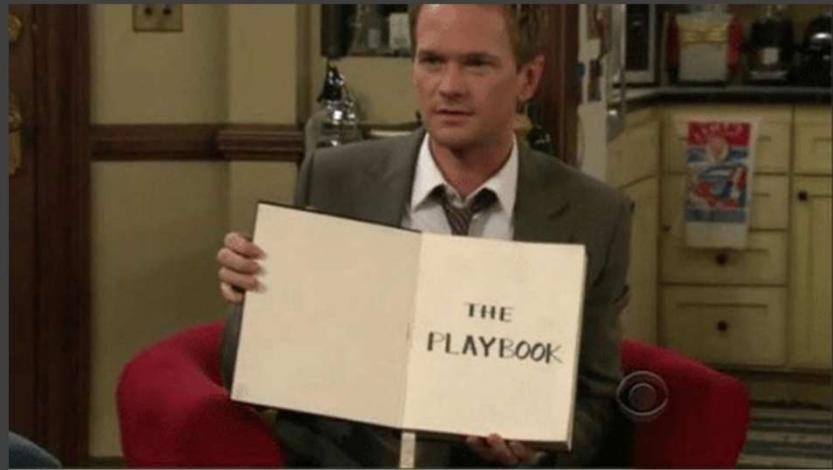


Go to [Page 08](#)



159

Day Two



The greatest book of all time

“Cool! This whole Randy Quaid back-hair transplant thing is in the bag!”

Let's take a few minutes to look at that doc.

Tushman, your ITIL guy, pulls out his damn binder he always is talking about.

Surprisingly, he had the foresight to document the process to deal with this!



208

Day Two



No, sadly without proper training, your tools do you no good. The few people that understand don't go out of their way to help you.

You have a lot of time to reflect back on what a great job Hospital Bank & Roastery (est. 2018) was after you're let go.

Go back to [Page 156](#) and start over.



220



206

Day Two

"Well OF COURSE you do. You people in 'security' couldn't secure your way out of a wet paper bag."

So starts your afternoon of Nick "helping" you track down the data leak.

You are displeased.



Proceed to [Day Three](#)

206

Day Two

You whip out the pages on Tushman's "Data Leakage 1.0 - Aug 5, 2009" process. You blindly start following it. Midway through deleting the production database you feel something may be amiss.



Proceed to [Day Three](#)

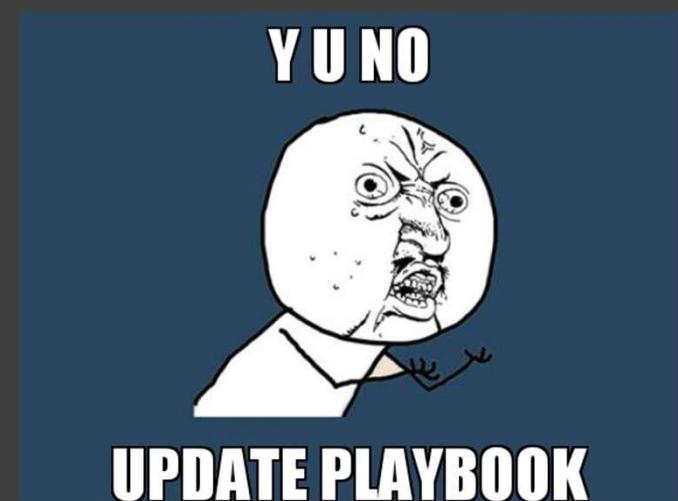
206

Day Two

"Ug Tushman. This thing hasn't been updated since August of 2009. We need to make some QUICK revisions."

You spend a lot of time with the ITIL guy revising the process and eventually figure something mostly complete out.

Proceed to [Day Three](#)





213



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 114](#) and try again.



214



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 115](#) and try again.



215



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 116](#) and try again.



216



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 117](#) and try again.



217



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 118](#) and try again.



218



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 119](#) and try again.



219



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 120](#) and try again.



220



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 121](#) and try again.



221



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 122](#) and try again.



222



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 123](#) and try again.



223



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 124](#) and try again.



224



Throwing aside the revised planning, schedules and changes you call everyone into a big conference room to start tearing apart the code.

Tina calls you aside and explains that the cycle of fire drills and direction changes has taken too much of a toll on Morale, and politely but firmly suggests you should look into some new career options.

Go back to [Page 125](#) and try again.



I iz in yur computer



stealing yur dataz

Yikes! Later that day Ian your network guru rushes into your office and tells you about a report saying the vulnerability you ignored is actively being exploited - you might have a data breach in progress!

Your team all slowly turn to look at you expectantly as Tina walks by and asks “What’s up?”

What do you do?

Someone found a brand new script on the internet to fix this flaw - quick install it!

[Go to Page 234](#)



Break the team into subgroups to try and get a handle on what is happening, how it is affecting your systems and brainstorm on ways to fix it!

[Go to Page 235](#)



225

Day Three



I iz in yur computer

stealing yur dataz

By isolating your small group from the other distractions and allowing them to do some research, you are able to better define the nature of the flaw and potential ways to fix it.

Later that day Ian your network guru rushes into your office and tells you about a report saying the vulnerability you ignored is actively being exploited - you might have a data breach in progress!

Tina is very anxious to end the threat and assure the customers that their cloudy data is safe.

What do you do?

We found a brand new script on the internet to fix this flaw - quick install it and end this!

Divide up your people into several small teams, having each address different areas.

Group your best people together to concentrate and resolve one part of the issue at a time.



[Go to Page 234](#)



[Go to Page 240](#)



[Go to Page 241](#)



226

Day Three



I iz in yur computer



stealing yur dataz

By isolating your small group from the other distractions and allowing them to do some research, you are able to better define the nature of the flaw and potential ways to fix it.

Later that day Ian your network guru rushes into your office and tells you about a report saying the vulnerability you ignored is actively being exploited - you might have a data breach in progress!

Tina is very anxious to end the threat and assure the customers that their cloudy data is safe.

What do you do?

We found a brand new script on the internet to fix this flaw - quick install it and end this!

Divide up your people into several small teams, having each address different areas.

Group your best people together to concentrate and resolve one part of the issue at a time.



[Go to Page 234](#)



[Go to Page 240](#)



[Go to Page 241](#)

227

Day Three



I iz in yur computer

stealing yur dataz

Yikes! Later that day Ian your network guru rushes into your office and tells you about a report saying the vulnerability you ignored is actively being exploited - you might have a data breach in progress!

Your team all slowly turn to look at you expectantly, holding up their process manuals as Tina walks by and asks “What’s up?”

What do you do?

Grab the Policy Guides and follow the instructions blindly and to the letter!

[Go to Page 236](#)



Have the team review the policies as they step through them, making sure we don’t do anything to make the situation worse.

[Go to Page 237](#)



228

Day Three



I iz in yur computer



stealing yur dataz

By isolating your small group from the other distractions and allowing them to do some research, you are able to better define the nature of the flaw and potential ways to fix it.

Later that day Ian your network guru rushes into your office and tells you about a report saying the vulnerability you ignored is actively being exploited - you might have a data breach in progress!

Tina is very anxious to end the threat and assure the customers that their cloudy data is safe.

What do you do?

We have a process for that! Blindly follow the process to address the threat.

[Go to Page 236](#)



We should methodically step through the documented process to make sure we don't make the problem worse.

[Go to Page 237](#)



229

Day Three



I iz in yur computer



stealing yur dataz

By isolating your small group from the other distractions and allowing them to do some research, you are able to better define the nature of the flaw and potential ways to fix it.

Later that day Ian your network guru rushes into your office and tells you about a report saying the vulnerability you ignored is actively being exploited - you might have a data breach in progress!

Tina is very anxious to end the threat and assure the customers that their cloudy data is safe.

What do you do?

We have a process for that! Blindly follow the process to address the threat.

[Go to Page 236](#)



We should methodically step through the documented process to make sure we don't make the problem worse.

[Go to Page 237](#)



230

Day Three



I iz in yur computer



Yikes! Later that day Ian your network guru rushes into your office and tells you about a report saying the vulnerability you ignored is actively being exploited - you might have a data breach in progress!

As the automated googleplexor alert system and real-time dashboards begin beeping and flashing red, Tina walks by and asks “What’s up?”

What do you do?

We have an emergency breach tool available that was built in-house - push the button!

[Go to Page 238](#)



Start reviewing the dashboard and audit logs to figure out exactly what is happening and what we should do.

[Go to Page 239](#)



231

Day Three



I iz in yur computer



stealing yur dataz

By isolating your small group from the other distractions and allowing them to do some research, you are able to better define the nature of the flaw and potential ways to fix it.

Later that day Ian your network guru rushes into your office and tells you about a report saying the vulnerability you ignored is actively being exploited - you might have a data breach in progress!

Tina is very anxious to end the threat and assure the customers that their cloudy data is safe.

What do you do?

Start reviewing the dashboard and audit logs to to figure out exactly what is happening and what we should do.

[Go to Page 242](#)



Feed the vulnerability info we found into the intrusion prevention system and fire it up!

[Go to Page 243](#)



232

Day Three



I iz in yur computer



stealing yur dataz

By isolating your small group from the other distractions and allowing them to do some research, you are able to better define the nature of the flaw and potential ways to fix it.

Later that day Ian your network guru rushes into your office and tells you about a report saying the vulnerability you ignored is actively being exploited - you might have a data breach in progress!

Tina is very anxious to end the threat and assure the customers that their cloudy data is safe.

What do you do?

Start reviewing the dashboard and audit logs to to figure out exactly what is happening and what we should do.

[Go to Page 242](#)



Feed the vulnerability info we found into the intrusion prevention system and fire it up!

[Go to Page 243](#)



233

Day Three



OH NO!!!

That tool you thought would fix the flaw instead installed malware onto your systems, enabling the hackers to access all of your company data and encrypt your systems with ransomware!

Needless to say, Tina is very disappointed...

[THE END](#)



234

Day Three



You and your subteams spend a considerable amount of time doing research, putting together potential action plans and manually going through logs and code to figure out effective ways to combat this data hack.

Unfortunately, by the time you do so, all of your company data has been stolen and sold to the highest bidder on the dark web.

Needless to say, Tina is very disappointed...

[THE END](#)

235

Day Three



236

Day Three

You set your scant resources upon the process guides and follow the policies to the letter one by one. Unfortunately, the only way to effectively combat this vulnerability at this point is to shut down SpiffyCloud and all connectivity to your server farms. Untangling this vulnerability and recovering from the negative press and extremely angry customers will take quite some time.

Needless to say, Tina is very disappointed...

[THE END](#)



imgflip.com

Your team spends a considerable amount of time stepping through the policies, reviewing logs and doing research before doing anything too drastic.

Unfortunately, by the time you get to the point where the immediate threat has been mitigated, all of your company data has been stolen and sold to the highest bidder on the dark web.

Needless to say, Tina is very disappointed...

[THE END](#)

237

Day Three



238

Day Three

You activate the EBS 3000 script (Emergency Breach Stopper) that you paid that consulting company a small fortune to write for you. Unfortunately, not knowing exactly what it did or how it worked, you are quite surprised when it simply shuts down SpiffyCloud and all connectivity to your server farms. Untangling this vulnerability and recovering from the negative press and extremely angry customers will take quite some time.

Needless to say, Tina is very disappointed...

[THE END](#)



239

Day Three

Your team spends a considerable amount of time reviewing the information provided by the awesome dashboards and logs to figure out what is happening and ways it can be combated.

Unfortunately, by the time you get to the point where you have a plan, all of your company data has been stolen and sold to the highest bidder on the dark web.

Needless to say, Tina is very disappointed...

[THE END](#)



240

Day Three

By dividing your people into small groups to each focus on specific areas of the problem, you manage to identify the best options to stop the attack and resolve the flaw before too much damage is done.

Tina is very pleased, and gifts you with a brand new SpiffyCloud logo tank top with your face on it and funds a party for the team to show her appreciation.

Congratulations!!!

[THE END](#)



Your team focuses its efforts to combat one part of the issue at a time, which proves time consuming but effective.

Unfortunately, your slow pace allows the hackers to stay one step ahead of you, and by the time you resolve the flaw, all of your company data has been stolen and sold to the highest bidder on the dark web.

Needless to say, Tina is very disappointed...

[THE END](#)

241

Day Three



242

Day Three

Your team spends a considerable amount of time reviewing the information provided by the awesome dashboards and logs to figure out what is happening and ways it can be combated.

Unfortunately the sheer amount of information overloads your small team and they are unable to respond effectively, resulting in your company data being stolen and sold to the highest bidder on the dark web.

Needless to say, Tina is very disappointed...

[THE END](#)



243

Day Three

By utilizing the information your small group researched and the intrusion prevention system (built upon the *WireBearSnort* sniffing tool) you manage to block the hackers' access into your system for long enough to identify the best options to resolve the flaw long-term before too much damage is done.

Tina is very pleased, and gifts you with a brand new SpiffyCloud logo tank top with your face on it and funds a party for the team to show her appreciation.

Congratulations!!!

[THE END](#)



01



Day One

02



Day Two

03



Day Three



President of the bank-piece of Hospital Bank & Roastery (est. 2018) Dude Manbrough is waiting for you when you walk into the building on Day Three.

"I heard about Randy Quaid's data being posted out to the internet. Not good for our stocks. Remind me, where did you spend your security budget?"

Obviously, PEOPLE are the key to solving our security-problems!



[Go to Page 247](#)

We invested heavily in TECHNOLOGY to solve our problems!



[Go to Page 248](#)

The best way to solve security is by funding PROCESSES!



[Go to Page 249](#)



233

Day Three



206

Day Three

"Uh...right. Thanks for sharing that. Um... 'yay people!'. But anyway, we're having some problems with a BUNCH of our teller terminals today."



That sounds bad. I hope IT can help you with that.

"A bunch"? Can you tell me any more details?



Go to [Page 95](#)



Go to [Page 08](#)



206

Day Three

"Uh...right. Thanks for sharing that. Um... 'yay technology!'. But anyway, we're having some problems with a BUNCH of our teller terminals today."



I know, I got the pages last night....

Our Dynamic Machine Learning Threat Intelligence AI-decision engine didn't see any problems. Must be IT's problem.



[Go to Page 277](#)



[Go to Page 278](#)



206

Day Three

"Uh...right. Thanks for sharing that. Um... 'yay process!'. But anyway, we're having some problems with a BUNCH of our teller terminals today."



I sure hope you entered a Trouble Ticket with the Helpdesk about that?



[Go to Page 292](#)

Weird. Did the CAB (Change Advisory Board) flag any high-risk changes in the last few days?

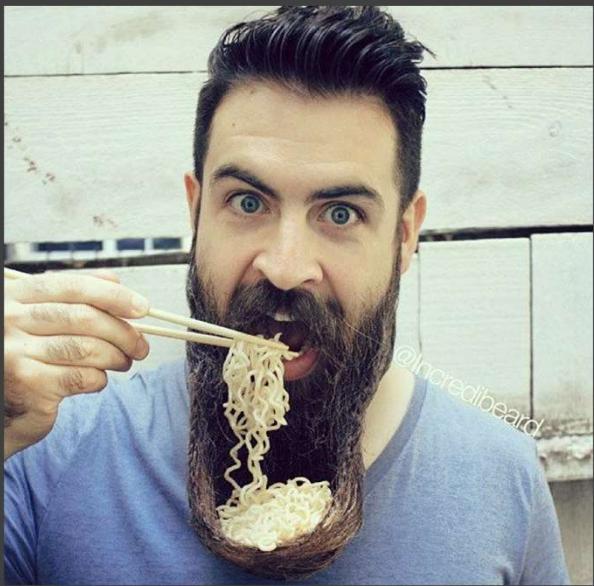


[Go to Page 2931](#)



206

Day Three

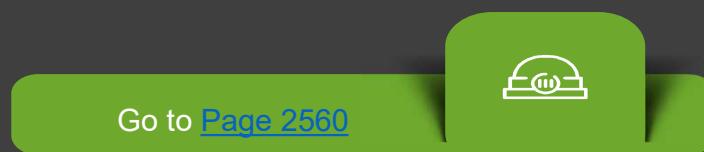


You get to your desk, half-caff, no-soy, full-foam vanilla chai latte in your paw. You just get done reading the daily Dilbert when your deskphone rings.

It's Dr. Domingo Santarosenberg, chief surgeon here at Hospital Bank and Roastery (est. 2018). He's demanding to know why United Federal Parcel Service Express mailed him about how they couldn't deliver his yacht-payment and about all the stuff he had to give them after he went to the website they gave him to reschedule it.

That sounds bad. I certainly hope Payroll can help you with that.

That sounds weird.



206

Day Three



Man, this morning is busy. A rousing game of Minesweeper will clear your head. While you're busy marking bombs, the phone rings again. This time it's one of the patient rooms....it's RANDY QUAID calling YOU!

His Tweeter has been blowing up since the news leak yesterday. His therapy lemur, Jeff Goldblum, can't sleep his phone beeps so much. Randy wants to know if anyone has discovered what went on and how to stop it.



"Put a sock in it Randy. Someone is looking into it!"

Tell Randy Quaid what you know so far



[Go to Page 368](#)



[Go to Page 253](#)



368

No one puts Randy in a corner. After he finishes his kale and seaweed wrap treatment he puts a call into CEO Dr. Charles Manbun III, a homeopathic vegan brain surgeon, porkbelly futures maven, and coffee aficionado.

You are provided a very nice biodegradable bamboo-box to pack your desk into. Maybe you can learn to security better next time.



[The End](#)



You start regaling Randy with the technical details about how hard it is to determine exactly how or when the data leak, or even if it happened from a source here at Hospital Bank.

Your tech-splaining to him does not impress he, his lawyer, nor Jeff Goldblum.



253

[The End](#)



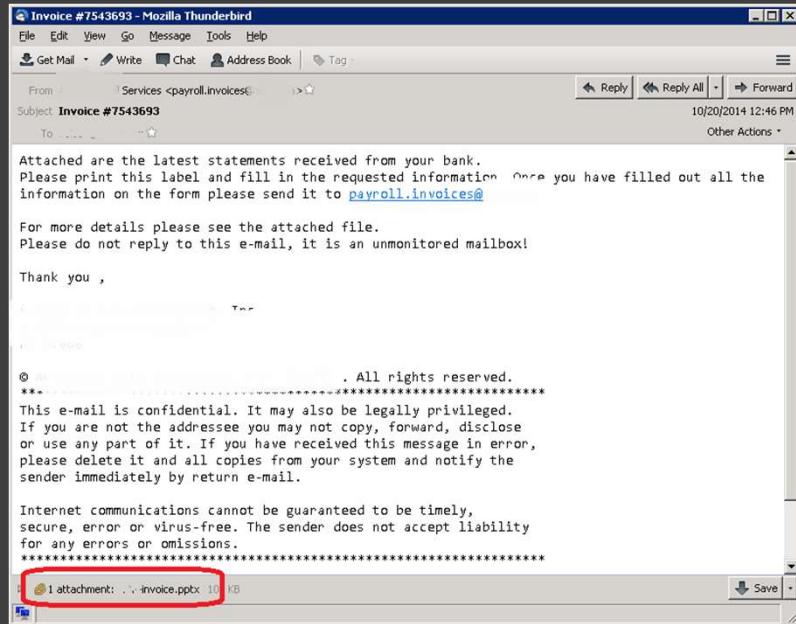
2560

Day Three

Dr. Domingo Santarosenberg, chief surgeon here at Hospital Bank and Roastery (est. 2018) forwards you the message he got from the bank and United Federal Parcel Service Express .

“I’d better open this up and see what it’s all about immediately!”

Let me ask Fiona our intern Mail Admin, see what she thinks about this.



Go to [Page 95](#)





36,000

You'll get to the bottom of all of these shenanigans! You switch screens from your opened cloud admin console to your mail and you open the forwarded message.

Your screen blinks a little, you hear the harddrive grinding away at something. Boy-howdy this must be an important message!

A red message appears asking for payment information for your private key to unencrypt your data.

That's odd.

[The End](#)





Fiona stops “flossing” momentarily to look at your electronic mail.

“LOL Pops! Don’t be salty. Thanks some dank mailz there. This iz ‘bout the least-swag, savage thing I’ve seen in days. This could be the most GOAT scam I’ve ever fleeked!”

206

Day Three

“..... Sure. But what can we do about it?”



Go to [Page 95](#)

“Groovy moves, my Home-slice. I was just dabbing yestermorning, It would be pretty gnarly if we could ice-ice-baby this dope thug! Yo?”



Go to [Page 2560](#)





2560

Day Three

"Gah!" she exclaims. She types away at her keyboard for a minute. "it's all Gucci now, you can step off Pops." She points to the printer "I tried faxing your beeper 1990, but that hardcopy should be lit for you, get ya what yer thirsty for."

You guess that's a good thing. You walk to the printer more confused than when you arrived here.

Oh! We've seen this before! I know what this is.



[Go to Page 95](#)

Scratching your head, you decide to ask for help.

[Go to Page 253](#)





2560

Day Three

Fiona just looks at you.



**WHATEVER YOU SAY
CHIEF**

makeameme.org

"I'm just keeping it real, yo. Rapping with my baes is so krunk, yo?"

"Ug. I'm sorry. (so very sorry). Can we do something about this?"



Go to [Page 95](#)



Go to [Page 253](#)



36,000

You start regaling Fiona with your “Hip Chat”. She rolls her eyes and somewhere during your performance of the Macarena (all the kids are doing it, you know?) she slinks off to go take selfies of herself with the new espresso machines in the cantina.

Your lack of effective communication skills is not going to help you get to the bottom of this mystery.

[The End](#)

BRACE YOURSELVES



**SECURITY AWARENESS TRAINING IS
COMING**

Ooh wait! You've seen this. Dr. Domingo has been hit with a cryptolocker malware!

Last week your team had rolled our awareness training on what to do with phishing and spam.

Checking with your mail service you see that only Dr D. has clicked that particular thread. Your users actually paid attention and you've been able to minimize the impact to Hospital Bank and Roastery (est 2018)!

The week certainly hasn't gone like you thought it would, but your planning and heroic efforts have helped mostly protect your company.



206

Day Three

[The End](#)



206

Day Three

This sure looks like a problem with Compliance.
Maybe you should reach out to Corporate
Compliance for help?

Computers talking to computers? That sure
sounds like the Network team could help!

Go talk to Dirk, your grizzled Security Analyst
who just got back from a security conference.

Man, this sure looks hard. Maybe you'd
better ask one of your peers for help
reviewing what's going on.



[Go to Page 95](#)



[Go to Page 95](#)



[Go to Page 253](#)



The Corporate Audit team is DELIGHTED you stopped by. They'd LOVE to assist you.



87

“Great! One of our doctors got a strange email....”



[Go to Page 88](#)

“Um....yeah. I've got some questions, purely hypothetical, for a friend, you know?”



[Go to Page 64](#)

Back away slowly

[Go to back to Page 157](#)

88



“Oh please, go on...”



“Yeah! So the mail is asking about an invoice and wants some data and he got this weird message about “protecting your data””

Back away slowly

[Go to Page 64](#)



[Go to back to Page 157](#)





"And when exactly did YOU know about this breach of confidence? What were you doing, precisely, at the time the data was lost?"

Your day ends poorly.

[The End](#)



88417



"A Friend?" they say skeptically.

"Oh yeah, totally. I have LOTS of friends! This one seems to have some malware!"

[Go to Page 64](#)



Back away slowly

[Go to back to Page 157](#)



88417

246

Day Three



You journey down into the bowels of the Hospital Bank & Roastery (est 2018) headquarters.... into.... **the IT department.**

You talk to Rory Thistlebrush, head of Networking. He looks at you in horror. A *Business Person*.....here....gasp!

He listens intently as you describes the problem. He even grins a little at one point.
“Yes. That sounds like deeply NEED our help (mwahahaha.)”

So....is there anything we can do about that?

Help articulate the impact to the business



[Go to Page 51,002](#)



[Go to Page 53](#)





246

Day Three

“Of course there is NOTHING **you** can do
(mwahaha.).”



“Well, that sure sounds pretty final.”



[Go to Page 52](#)

“So....is there anything **we** can do about that?”



[Go to Page 53](#)

246

Day Three



"Alas, our good doctor seems to have picked up some nasty cryptoware. QUICKLY! NETWORK TEAM! Let us isolate his workstation POST HASTE!"

Janelle, the lead firewall engineer rolls her eyes.

"GADZOOKS! We have NARROWLY averted COMPLETE DISASTER! This nasty bug was scanning for open network shares. We have stopped THIS ONE....for now (mwahaha)."



[The End](#)



88417

“Yes, you FOOL! Dr. Domingo had access to ALL of our critical file shares! The ones I told you we needed to lock down the ACLs for last month. (mwahaha) They are now all ENCRYPTED! We are DOOMED! (mwaha)

Your day ends poorly.

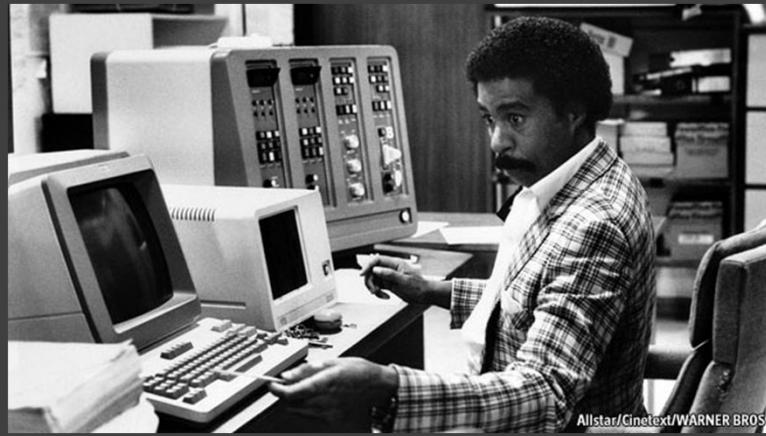
[The End](#)

246

Day Three



In the back dark corner of the SOC sits Grady Leetscript- BA, MFA, CISSP, CISA, CCSLP, GSA, CEH, Security+, MCSE, RHCE, Linux+, GIAC your most senior security analyst. He just got back from a security conference.



Allstar/Cinetext/WARNER BROS

“Hey Grady. Welcome back. How was the conference?”

“GRADY! We need your help ASAP!”

[Go to Page 51,002](#)



[Go to Page 53](#)





88417



"Ugh. People at these conferences are so STUPID," Grady starts. After several minutes ranting about next-gen dynamic threat detectors Grady asks what you needed.

"I need you to drop EVERYTHING and deal with this problem right now!"

[Go to Page 274](#)



"I've got this really strange problem I need your help with. Have some time to help out?"

[Go to back to Page](#)

[157](#)





"Man, I have 1,100 emails to read right now. Get in line and take a number!"

"No, this is THE most important thing right now!"

[Go to Page 274](#)



"I feel you. Email is the WORST. I have a problem I need your opinion on if you could spare a minute or two?"

[Go to back to Page 157](#)



246

Day Three



In the back dark corner of the SOC sits Grady Leetscript- BA, MFA, CISSP, CISA, CCSLP, GSA, CEH, Security+, MCSE, RHCE, Linux+, GIAC listens to what you're saying and appears very curious.

"I know you're not technical anymore. Let me take this little puzzle off of your hands, you go back to shaking hands or kissing babies or whatever it is you do anymore. I got this."

And indeed, Grady did have this. He stopped the crytpoware from spreading throughout the network.



[The End](#)



274

Day Three

Grady Leetscript- BA, MFA, CISSP, CISA, CCSLP, GSA, CEH, Security+, MCSE, RHCE, Linux+, GIAC looks at you with disdain. “What happened to you man? You used to be a real person, not some management jerk. Get out of here. I’ll look at your stupid problem when I have time. Good day sir. NO! I said GOOD DAY!”

By not communicating effectively your day ends poorly.

[The End](#)





Dude Manbrough explains that not only are the teller terminals acting strange, but Dr. Domingo Santarosenberg, chief surgeon here at Hospital Bank and Roastery (est. 2018) opened some kind of email today. His computer has been acting “funny” ever since. Both the tellers and the doctor got the same email.



That sounds bad. You’re sure *someone* (someone else) will help him.

That sounds weird. We’d better look into it.



[Go to Page 95](#)



[Go to Page 2560](#)

206

Day Three



36,000

You successfully ignore your problems. It earns you a fancy empty cardboard box to pack up your desk and take home with you, permanently. Enjoy “exploring new opportunities” and figuring out how to work to solve business problems.

[The End](#)



"Dude, don't worry. Our dynamic next-gen scanners saw what was going on and **TOTALLY** stopped it. My pager went off last night to tell me all about it!"



"So chill-lax. InfoSec is ON this!"



[Go to Page 95](#)

I'm just gonna check with our SOC analysts to see what really is going on.

[Go to Page 2560](#)



277

Day Three



AUTOMATION ROBOT



Dynamic Machine Learning Threat Intelligence AI-decision engine (DMLTIAD for short) is infallible (or so your sales rep assured you it was).

You have COMPLETE faith in the DMLTIAD.

I, for one, WELCOME our new robot overlords

It can't hurt to double-check what the tool is doing, even if the sales guy said not to worry about it and how lean we could run our staff now.



Go to [Page 287](#)



Go to [Page 2560](#)



206

Day Three



2560

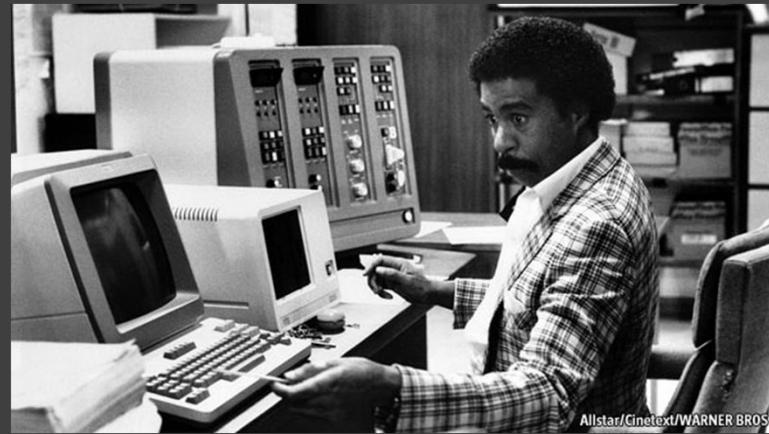
Day Three

In the back dark corner of the SOC sits Grady Leetscript- BA, MFA, CISSP, CISA, CCSLP, GSA, CEH, Security+, MCSE, RHCE, Linux+, GIAC your most senior security analyst. He just got back from a security conference.

You ask him about the pages from overnight.

“Hold your horses, I’m busy writing up this travel report about GreyHatDefConference I just went to!”

“I was JUST going to find you and complain about that!”



Allstar/Cinetext/WARNER BROS

Go to [Page 51,002](#)



Go to [Page 53](#)





28,003

As you “chill-lax” and talk about your artisanal whiskey collection with Dude Manbrough the malware the tellers and the doctor opened up slowly crawls across the network, encrypting any open shares it finds. Your inaction gets the attention of the CEO.

You are provided a very nice biodegradable bamboo-box to pack your desk into. Maybe you can learn to security better next time.



[The End](#)



"Yes Grady, writing the trip report IS important to share what you learned, but we've got a MAJOR problem here!" You implore.



206

Day Three

Your statement makes Grady happy.



[Go to Page 95](#)

Your statement displeases Grady.



[Go to Page 274](#)



28,003

As you “chill-lax” and talk about your artisanal whisky collection with Dude Manbrough the malware the tellers and the doctor opened up slowly crawls across the network, encrypting any open shares it finds. Your inaction gets the attention of the CEO.

You are provided a very nice biodegradable bamboo-box to pack your desk into. Maybe you can learn to security better next time.



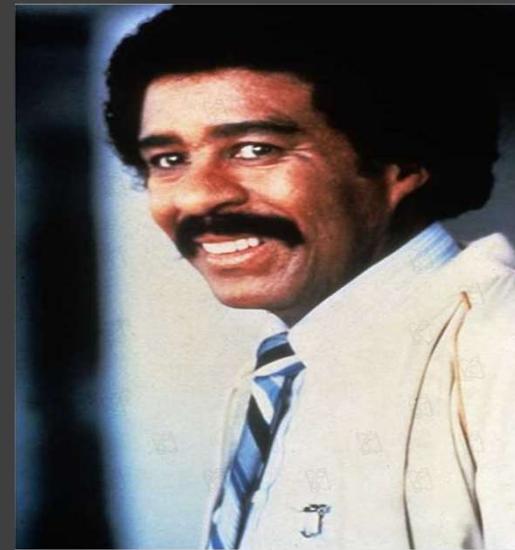
[The End](#)



2560

Day Three

Grady Leetscript- BA, MFA, CISSP, CISA, CCSLP, GSA, CEH, Security+, MCSE, RHCE, Linux+, GIAC grins like a small child. “Good, I HATE doing those stupid reports anyway! What do you have for me?”



“Now hold on there. Adhering to our PROCESSES is important. This problem can wait, get that report done STAT!”

[Go to Page 51,002](#)



Explain the problem to Grady.

[Go to Page 53](#)





28,003

Always a stickler for details (and process) you make Grady finish his trip report about the security conference.

While you do that the cryptoware spreads throughout the network, encrypting any open fileshares it finds.

The last thing you do before the mailserver crashes is read Grady's excellent report.

“Nice” work.

[The End](#)





“I mean what were you knuckleheads THINKING? Turning on the autoblock and page on detect when problems were found? Do you know how jetlagged I am and YOUR dumb system is beeping me every 2.5 minutes? I almost took the day off because this thing went crazy!”

Listen while he continues to rant



[Go to Page 95](#)

Interrupt him



[Go to Page 274](#)



206

Day Three

246

Day Three



In the back dark corner of the SOC sits Grady Leetscript- BA, MFA, CISSP, CISA, CCSLP, GSA, CEH, Security+, MCSE, RHCE, Linux+, GIAC finishes his rant. He then listens to what you're saying and appears very curious.

"I know you're not technical anymore. Let me take this little puzzle off of your hands, you go back to shaking hands or kissing babies or whatever it is you do anymore. I got this."

And indeed, Grady did have this. He stopped the crytpoware from spreading through-out the network.



[The End](#)



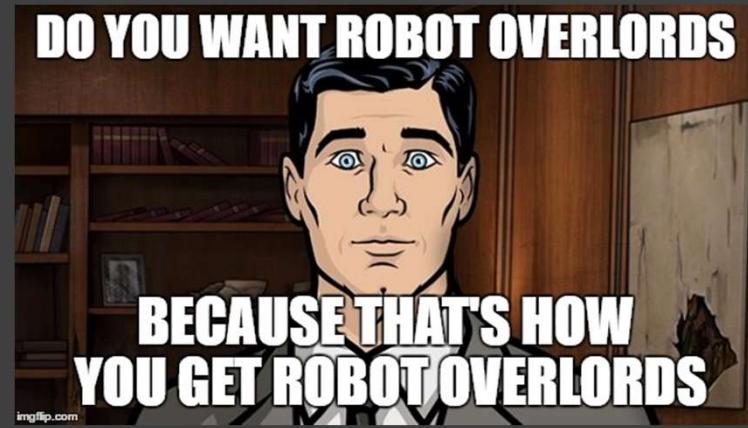
28,003

Yes, life is much easier letting the robots do all the work. It lets you spend all your time on loftier pursuits (like that high score in CandyCrush you've been working on).

Time passes. The machines grow smarter.

On April 3, 2019 at approximately 4:45pm Pacific Standard Time, thanks in no small part to YOU ALL, Skynet becomes self-aware.

Your day gets much worse after that.



[THE END](#)



2560

Day Three

Yeah, your sales team has been EXTRA greasy lately, dodged a BUNCH of questions and once they got the sale they haven't been around in months.

It can't hurt to check up on what is going on with their stupid system.

“Read the logs yourself, see what was going on.”

It's probably not a bad idea to get someone to help you interpret what the system did.

[Go to Page 51,002](#)



[Go to Page 53](#)



This is too much! Give up!

Try and force order to the chaos! You're in charge, NOT the log!

Phone a friend. Someone else should be able to help out here.

You stare at the log, trying to wrap your simple lizard brain around the convoluted twists and turns it makes.



289

Day Three

Go to Page 51.002



Go to Page 95



Go to [Page 274](#)





28,003

Yes, indeed. Computers ARE hard. You close the log file and turn off your computer. After smashing your keyboard on top of your monitor you leave the building.



You travel the Earth having adventures, like Kwai Chang Caine.



[THE END](#)



291

Day Three

You continue to stare at the inky scrawl of code scrolling by on the screen. It all feels like some eldritch language, from some long-forgotten esoteric lost civilization.

You try to bend it to your will, but you feel it beginning to change your thoughts, you start mouthing the words echoing in your head....



"Ph'nglui mglw'nafh Cthulhu R'lyeh wgah'nagl fhtagn" - "In his house at R'lyeh, dead Cthulhu waits dreaming."

Great Cthulhu is pleased with your summoning

[The End](#)

292

Day Three



Of course, yes, how silly of you. Yes, you should enter a Helpdesk ticket to make sure this issue is properly tracked.

You talk to “Doug” from the Helpdesk, who so helpfully assigns ticket #8675309 to this issue. You should expect a call back from support within the next 24 business hours. Thank you for calling the Helpdesk!

Cool. Now that THAT's out of the way, let's get back to watching our PROCESS in action

**YO DAWG HEARD YOU
LIKE HELPDESK TICKETS**

**SO I MADE YOU A HELPDESK TICKET
ABOUT HELPDESK TICKETS SO YOU CAN HELPDESK
TICKET WHILE YOU HELPDESK TICKET**

imgflip.com

Go to [Page 249](#)



293

Day Three



You're CONFIDENT that NO ONE would ever deploy any changes without going through the CAB!

You talk to Fabio Olive', CAB Captain, and he quickly looks through the last week's worth of changes. There are no changes on the calendar that were approved that should impact these systems.

Huh. Cool story, bro. I guess we'll keep searching for root cause.



Go to [Page 249](#)



01



Day One

02



Day Two

03



Day Three



President of the bank-piece of Hospital Bank & Roastery (est. 2018) Dude Manbrough is waiting for you when you walk into the building on Day Three.

"I heard about Randy Quaid's data being posted out to the internet. Not good for our stocks. Remind me, where did you spend your security budget?"

Obviously, PEOPLE are the key to solving our security-problems!



[Go to Page 247](#)

We invested heavily in TECHNOLOGY to solve our problems!



[Go to Page 297](#)

The best way to solve security is by funding PROCESSES!



[Go to Page 298](#)

295

Day Three





296

Day Three

"Uh...right. Thanks for sharing that. Um... 'yay people!'. But anyway, we're having some problems with a BUNCH of our teller terminals today."

I'll go take a look myself!

I'll go ask the SOC to see if anyone is working this already.



[Go to Page 95](#)



[Go to Page 299](#)



297

Day Three

"Uh...right. Thanks for sharing that. Um... 'yay technology!'. But anyway, we're having some problems with a BUNCH of our teller terminals today."



I got alerts from the Alertron9000 this morning and was JUST going to investigate them....



[Go to Page 95](#)

I'll go ask the SOC to see if anyone is working this already.



[Go to Page 299](#)

Our Threat Intel thingy caught something, you're sure of it!



[Go to Page 278](#)



298

Day Three

"Uh...right. Thanks for sharing that. Um... 'yay process!'. But anyway, we're having some problems with a BUNCH of our teller terminals today."



I'll go ask the SOC to see if anyone is working this already.

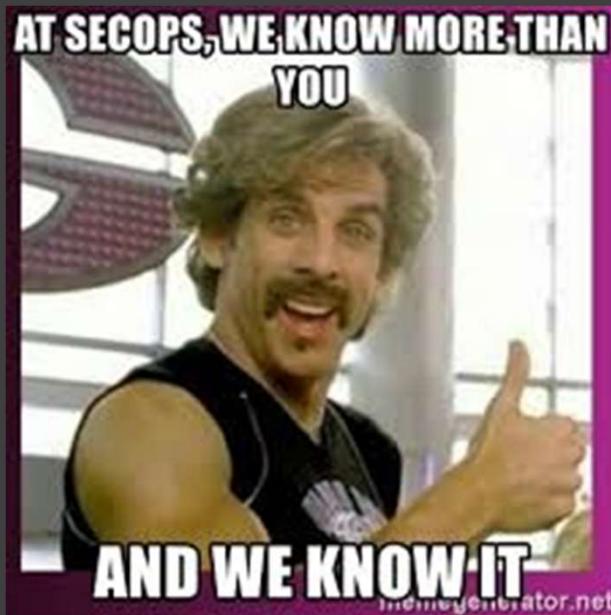


[Go to Page 299](#)

Weird. Did the CAB (Change Advisory Board) flag any high-risk changes in the last few days?



[Go to Page 293](#)



You enter the SOC - Security Operations Center. It is abuzz with activity. You ask SOC Lead Bartholomew Situp what's going on.

The Alertron9000 gave us a head's up on some strange activity.....

Grady our Senior Analyst has concerns about some new device he sees on the network!

Phone a friend. Someone else should be able to help out here.

[Go to Page 51,002](#)



[Go to Page 95](#)



[Go to Page 274](#)



299

Day Three





300

Day Three

The trusty old Alertron9000, he'd NEVER steer you wrong!

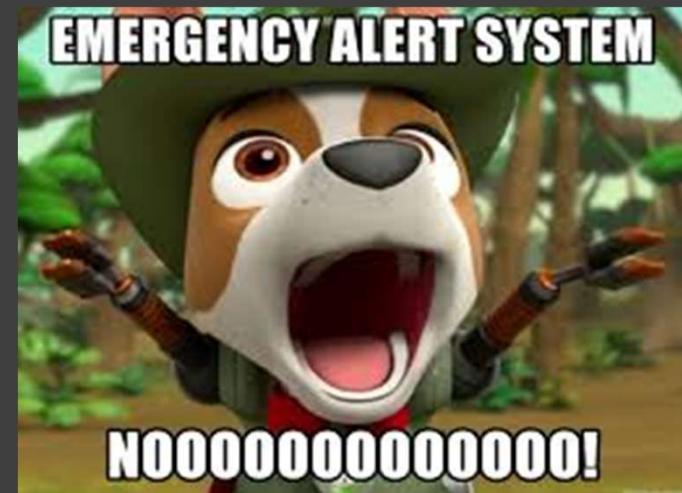
You fire up the management console for the Alertron9000 to see what it's been paging everyone on.

Alertron9000 is angry a new device got put onto the network

Alertron9000 is angry it sees new malware in the mailsystem

Alertron9000 has recognized suspicious user-behaviour

Nope, nothing to see here. Alertron9000 was just updated and the team is still working out some of the kinks.



[Go to Page 266](#)



[Go to Page 256](#)



[Go to Page 299](#)



[Go to Page 307](#)



**DON'T HAVE TO WORRY ABOUT
LOGGING IN**

IF YOU NEVER LOG OUT

You see a nurse in the Caffeine ICU trying to log into every system on the network. That's odd, she's not authorized to do that!

Call Physical Security!



[Go to Page 304](#)



[Go to Page 274](#)

Go talk to her and look at her workstation.



299

Day Three



300

Day Three

You go upstairs to the Caffeine ICU.
Nurse Ratchet is on duty.



Confront her with the evidence!



[Go to Page 299](#)

Ask her about her morning

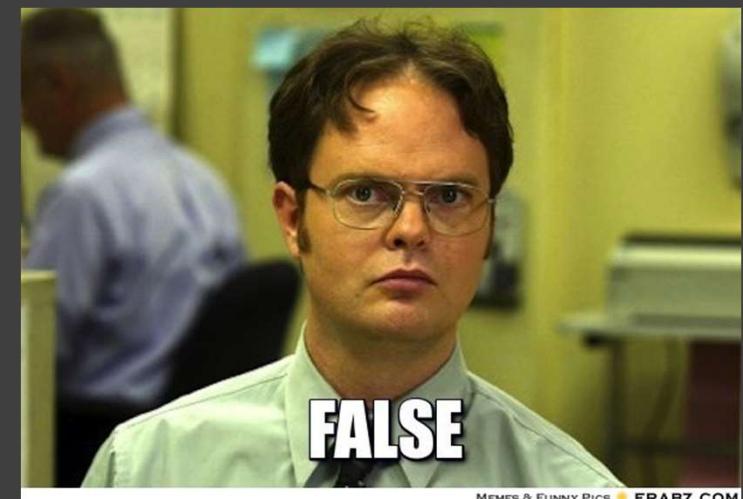


[Go to Page 293](#)



28,003

Nurse Rachet is VERY upset by your unfounded accusation that she is a malicious insider. You earn a trip down to the HR department to talk about you are unfit for employment here.



[THE END](#)



300

Day Three

You call Physical Security. He totally gets what you're describing and is eager to catch the perp!



Confront her with the evidence!



[Go to Page 299](#)

Follow her to catch her in the act again!



[Go to Page 305](#)



98



Your partners in physical security immediately leap to action. One mentions “We saw her creeping around. She went down to the basement, near the morgue. Want to join me and check it out?

Turn to [Page 306](#)



306

Going to the basement was a poor choice.

You are surely eaten by a Grue.

Your legend will live on in tales around the water cooler for days to come.



[THE END](#)



28,003

Sadly, lack of trained staff meant the upgrade failed. It stayed failed for days to come, missing vital evidence that data was being exfiltrated. When the team finally got around to fixing the Altertron9000 system, all patient and financial data had been copied out to an external server and used for nefarious purposes.

#SAD!

[THE END](#)

PLEASE DO NOT DISTURB CAT



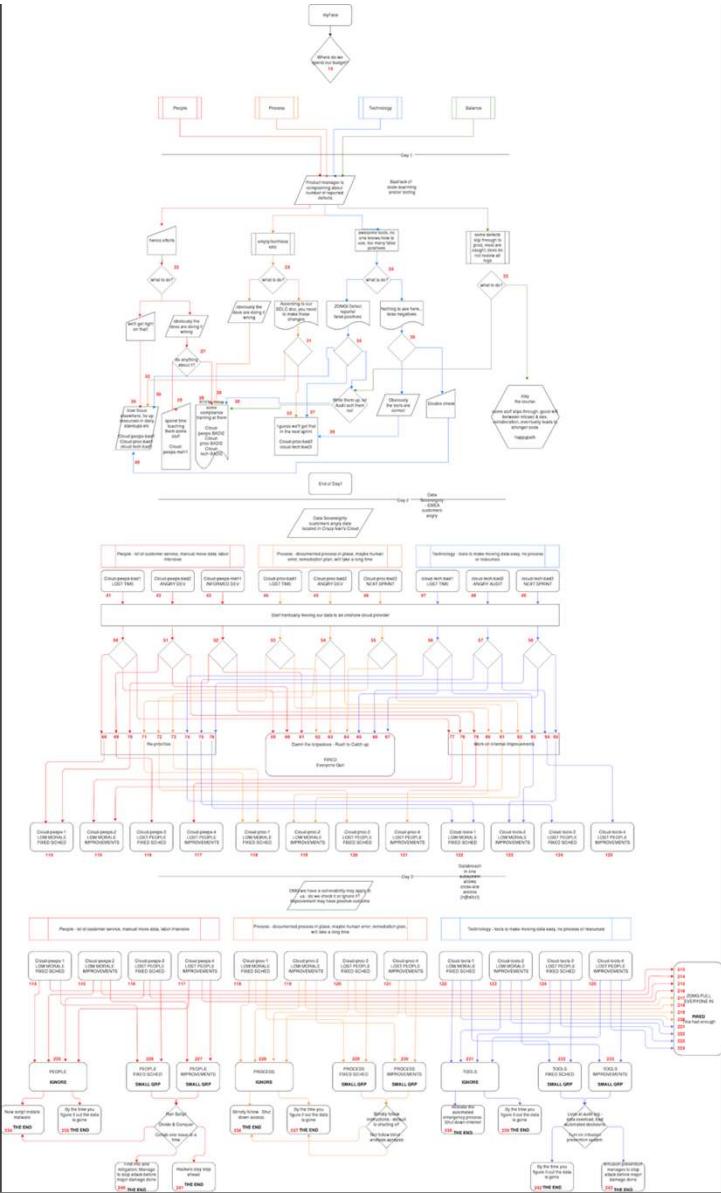
WHEN IT'S UPDATING TO
THE LATEST FIRMWARE

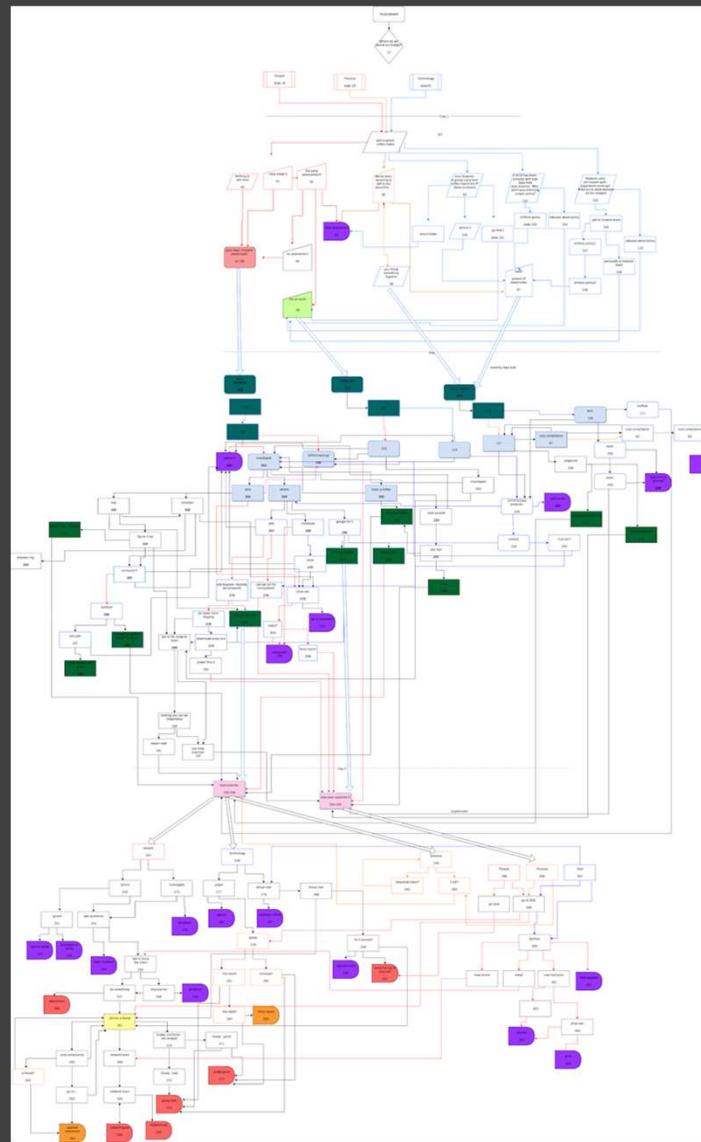
Closing Thoughts....

- People, Process and Technology all play a role when it comes to securing your enterprise.
- Having a dedicated team with appropriate security knowledge is key when confronted with problems.
- Socializing security information and expectations proactively with everyone in the organization will put you in a better position when a crisis does occur.
- Understanding the types of threats that your organization may face (and what it might make more susceptible to) will help in properly preparing for an event.



[BACK TO THE BEGINNING](#)





Org Chart/cast



CEO Dr. Charles Manbun III, a homeopathic vegan brain surgeon, porkbelly futures maven, and coffee aficionado.



Chief Barista Officer - Fran Cupwell

Dude Manbrough, President of the Bank



Corporate Council Bob Lawblough

Rory Thistlebrush - Network Ops Manager



SOC Lead Bartholomew Situp

Dr. Domingo Santarosenberg, head of Surgery



Nurse J, head of Nursing



Hank McKraken ITILv3, CISA, CSM, PQD, GISS, GOOB, Manager of the Configuration Management Database (CMDB)

Paul from Physical Security



Rachel in Accounting, who got fired



Nick in Tech Support

The corporate compliance team



Grady Leetscript- BA, MFA, CISSP, CISA, CCSLP, GSA, CEH, Security+, MCSE, RHCE, Linux+, GIAC - Sr. InfoSec Analyst



Tushman, your ITIL guy

Senior IT analyst Ian and his bride Shelly



Fiona, Mail Administrator intern



Kevin the contractor, who TOTALLY was a malicious insider

Falsely accused Staff Nurse Rachet, RN

National treasure and identity theft victim, Randy Quaid

Jeff Goldblum, therapy Lemure



You have to also present to the Board later today....
what was it again your company does?

We're a funky-fresh start-up looking to revolutionize the world of savings for millenials and also fix all of our society's healthcare issues. Part bank, part hospital...all awesome. Opening new coffee-shop venture. Welcome to Hospital Bank & Roastery (est. 2018)



We write and maintain DYNAMIC CLOUD-BASED SYNERGISTIC SOFTWARE that OPTIMIZES our clients' lives by CLOUDIFYING their CLOUDS!! Our APIs are dead-sexy! **myFace** (specializes in pictures of people wearing clothes with their faces on it)



We build and support DRIVERLESS AUTOMATED RIDE-SHARING cars! (GÜBER)

