

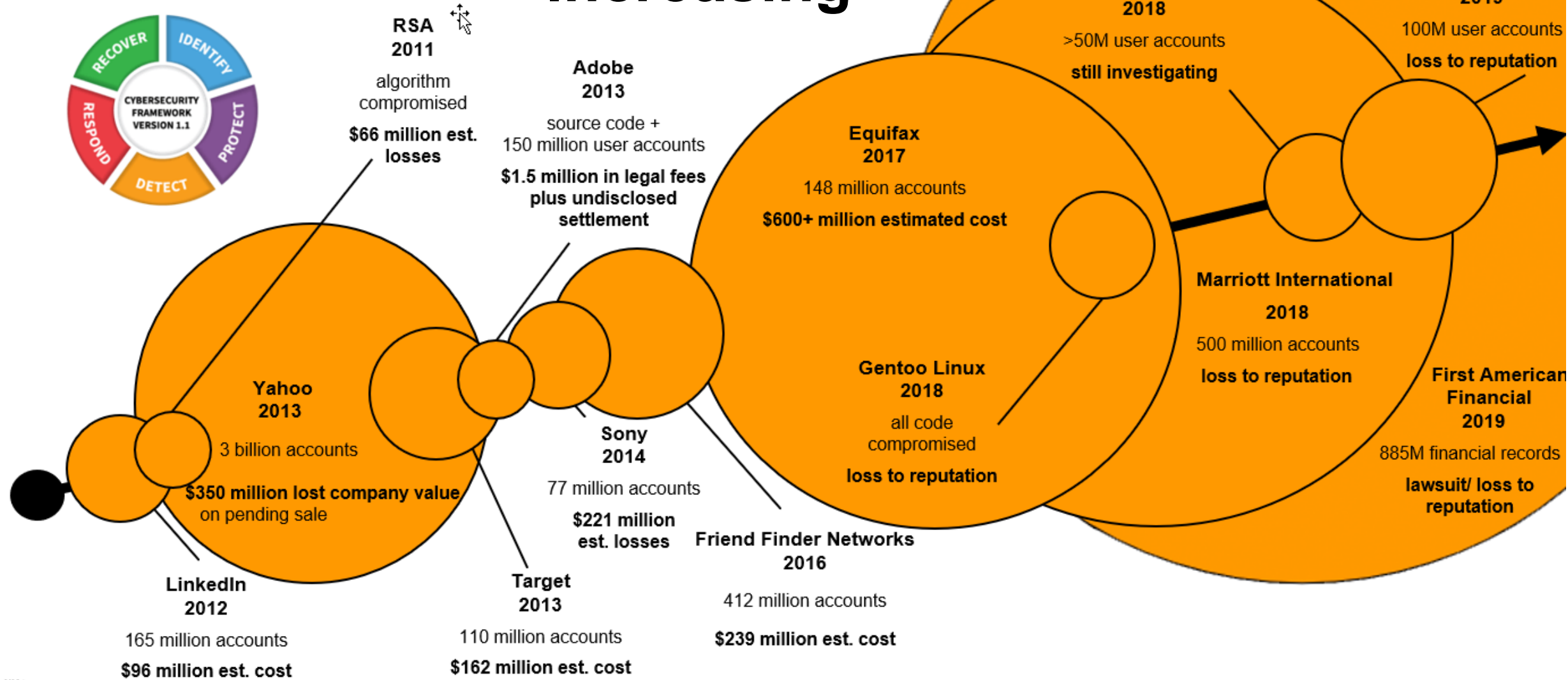
Cybersecurity Landscape

*Fiduciary leadership of Cybersecurity
through Strategy & Governance*

July 2019 | Version 3.0



Customer Data Breaches: Impact and Severity Increasing





```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61F758JSESSIONID=SD5SL4FF1AD0FF9 HTTP 1.1" 404 720 "http://buttercup-9
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7F6AD0FF9 HTTP 1.1" 200 1318 "http://buttercup-shop
" 317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-268JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shop
ows NT 5.1: SV1: - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-268JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shop
itemId=EST-168&product_id=RP-LI-02" 468 125 17 / "GET /category.screen?category_id=SD5SL9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shop
:/buttercup-shopping_id=RP-LI-02" 468 125 17 / "GET /category.screen?category_id=SD5SL9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shop
toaction=purchase&id=com/est-268JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shop
opping.com/c/est-268JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 404 3322 "http://buttercup-shop

```

“I liken it to the very first aero-squadron, when they started with biplanes. We’re at the threshold of a new era... we are not exactly sure how combat in this new dimension of cyberspace will unfold. We only know we’re at the beginning.”

“Few if any contemporary computer security controls have prevented a red team from easily accessing any information sought.”

“The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.”

“Computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses... account for the largest portion of economic and industrial information lost by US corporations.”

“Espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations... and are insulated from risks of internationally embarrassing incidents.”

“The almost obsessive persistence of serious penetrators is astonishing.”

“I almost feel like it’s the early days of flight with the Wright brothers. First of all, you need to kind of figure out that domain, and how are we going to operate and maintain within that domain. So I think it will take a period of time, and it’s going to be growing.”

“Our red teams do get into most of the networks we target.”

“I liken it to the very first aero-squadron, when they started with biplanes. We’re at the threshold of a new era... we are not exactly sure how combat in this new dimension of cyberspace will unfold. We only know we’re at the beginning.” - **1996**

“Few if any contemporary computer security controls have prevented a red team from easily accessing any information sought.” - **1979**

“The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.” - **1981**

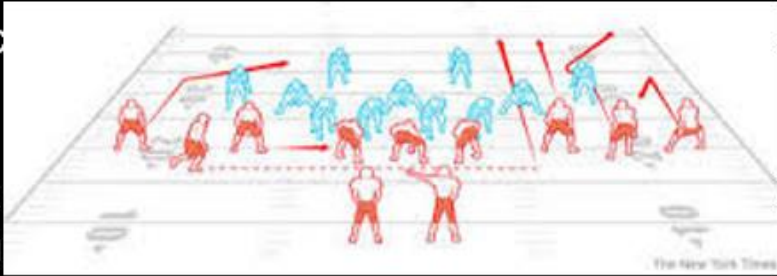
“Computer intrusions, telecommunications targeting and intercept, and private-sector encryption weaknesses... account for the largest portion of economic and industrial information lost by US corporations.” - **1995**

“Espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations... and are insulated from risks of internationally embarrassing incidents.” - **1988**

“The almost obsessive persistence of serious penetrators is astonishing.” - **1988**

“I almost feel like it’s the early days of flight with the Wright brothers. First of all, you need to kind of figure out that domain, and how are we going to operate and maintain within that domain. So I think it will take a period of time, and it’s going to be growing.” - **2009**

“Our red teams do get into most of the networks we target.” - **2008**

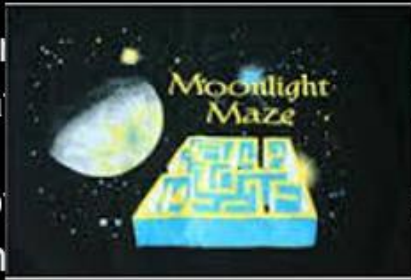


not work
growth in threats to system

water system

to match the apparent

“Computer intrusions, telecommunications targeting the largest portion of economic and industrial information... private-sector businesses... account for the



“Espionage over networks can be cost-efficient, or insulated from risks of internationally embarrassing results, and are



"Our red teams do get into most of th

Why?

Why are you doing this?

Why are you changing?

No plan survives first contact with the enemy

1st vs 2nd vs 3rd vs 4th gen war

How does the board support the 1.9M members?

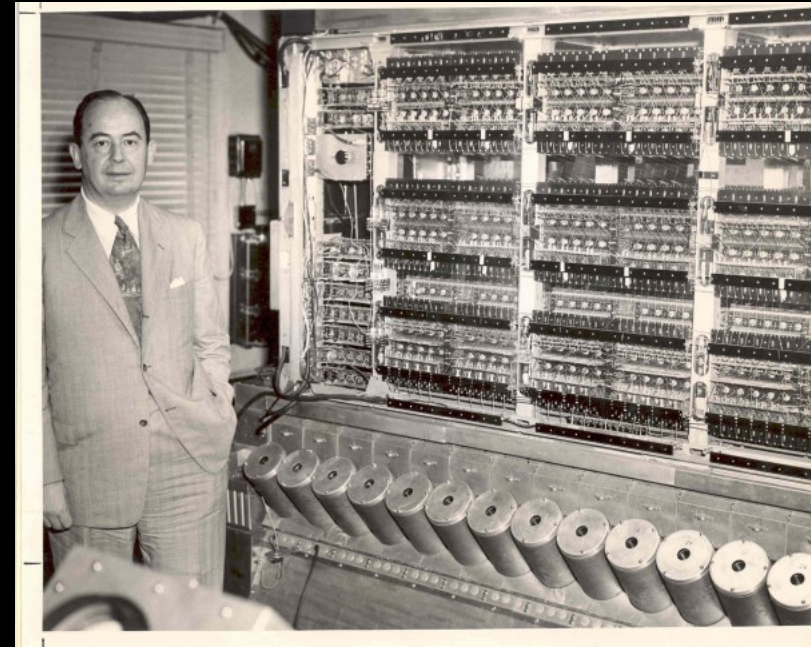
Use good examples from known good board members

Investment corporate governance -- how would you look to your own review?

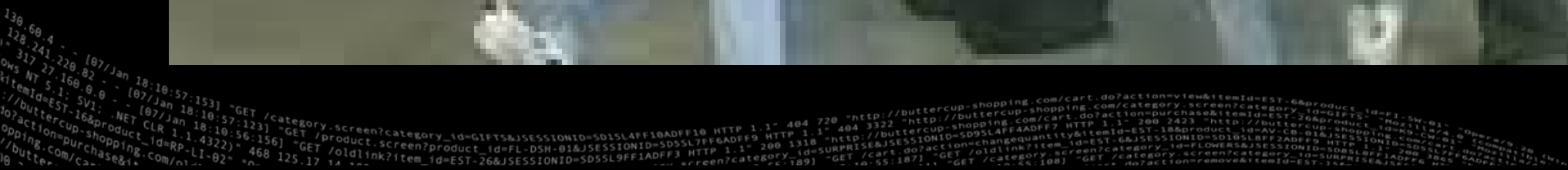
What level of breach are you ok with?

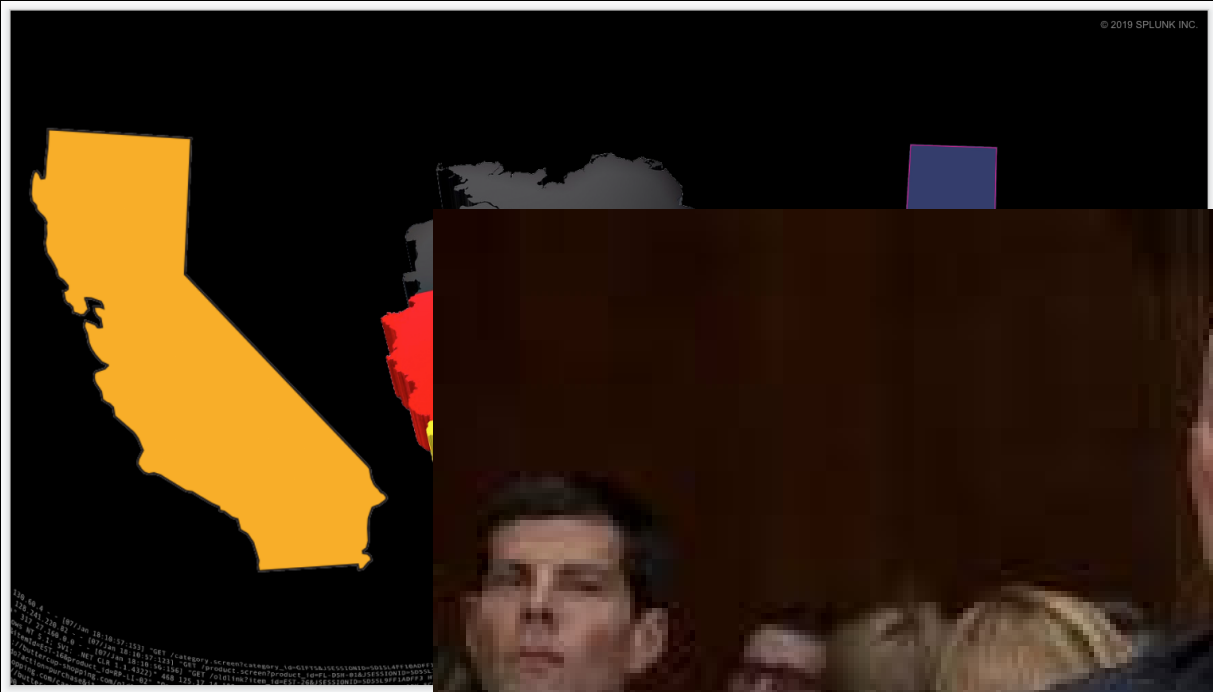












```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/purchase&itemId=EST-16&product_id=RP-LI-02" 125.17 14 1000
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/purchase&itemId=EST-16&product_id=RP-LI-02" 125.17 14 1000
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17 14 1000
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/purchase&itemId=EST-16&product_id=RP-LI-02" 125.17 14 1000
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/purchase&itemId=EST-16&product_id=RP-LI-02" 125.17 14 1000
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 468 125.17 14 1000
```



2880

5 dead after taking Tylenol capsules filled with cyanide

Close-to-home deaths trigger wave of fear

the company's new business strategy. The company's new business strategy is to focus on the high-end market, which is a market with a high growth rate and a high profit margin. The company's new business strategy is to focus on the high-end market, which is a market with a high growth rate and a high profit margin.



A string of coincidences linked Tylenol poisoning

1910

```

139.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=SD5LAFFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=GIFTS-16&quantity=1"
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3318 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-18&product_id=AV-CB-01&quantity=1"
ows NT 5.1: SV1 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-14&product_id=FI-SW-01"
item_id=EST-16&product_id=RP-LI-02" 468 125.17.14.100 "GET /category.screen?category_id=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-14&product_id=FI-SW-01"
do?category_id=RP-LI-02" 468 125.17.14.100 "GET /category.screen?category_id=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-14&product_id=FI-SW-01"
opping.com/purchase&item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-14&product_id=FI-SW-01"
0/buttercup-shopping.com/purchase&item_id=EST-26&SESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-14&product_id=FI-SW-01"

```

splunk  listen to your data®



2880

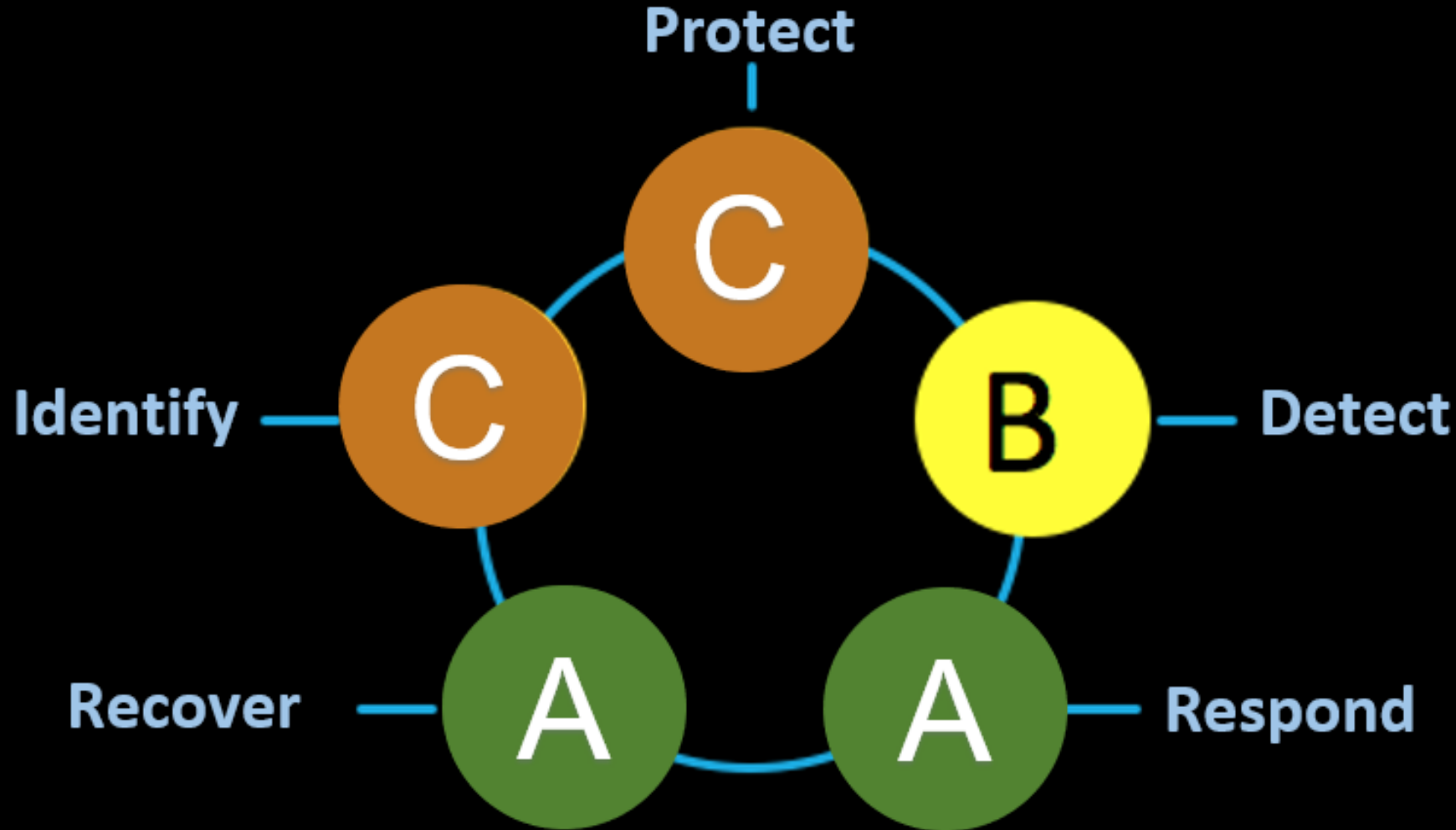


1910

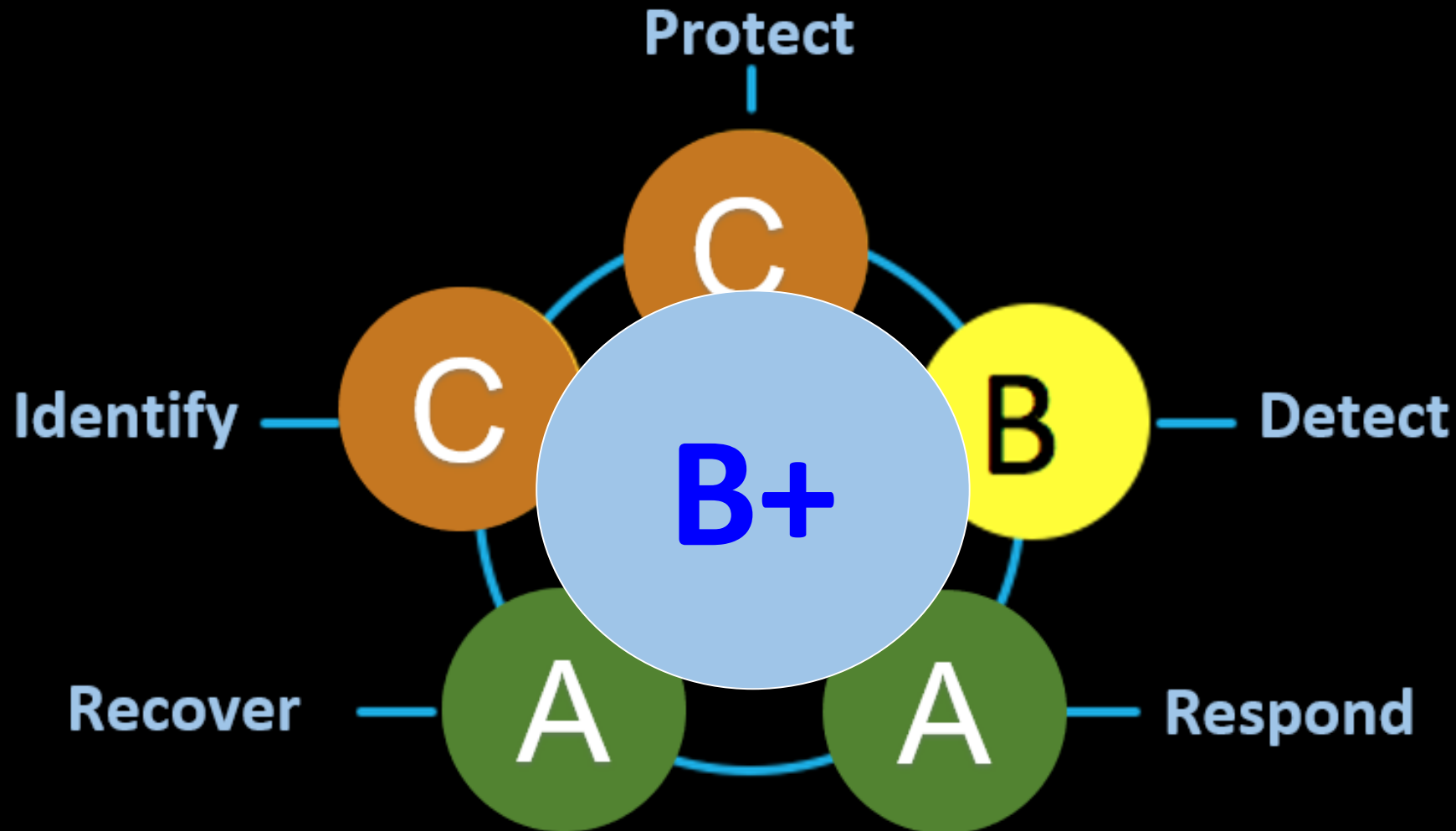




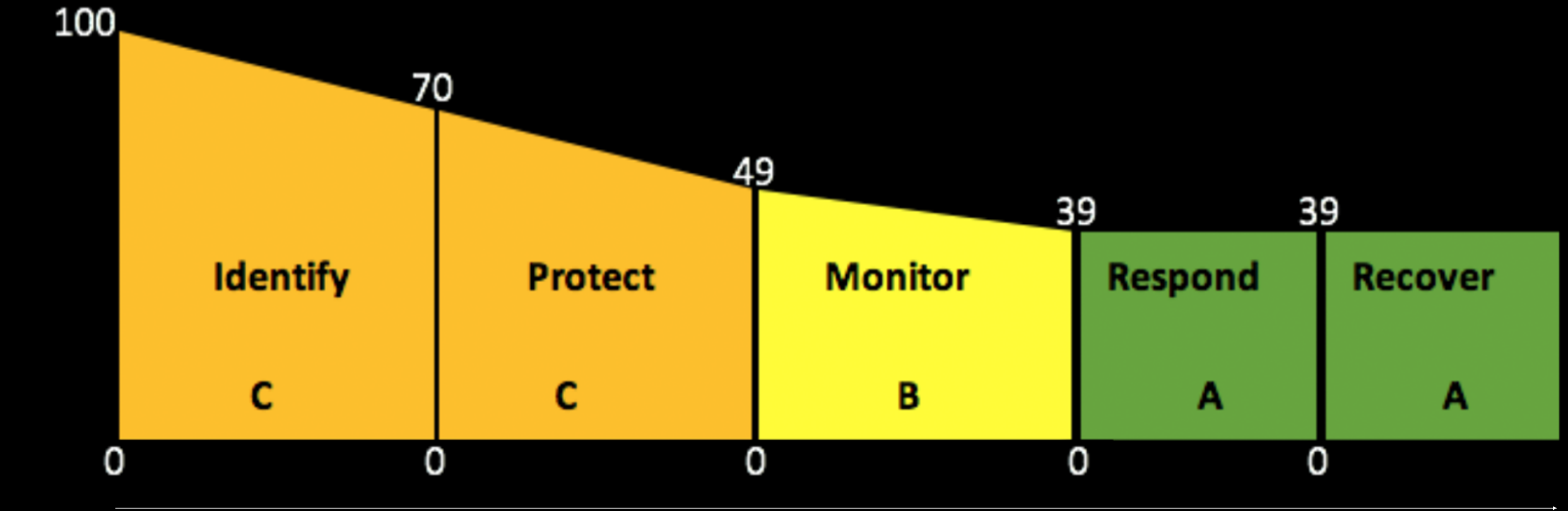
NIST Framework



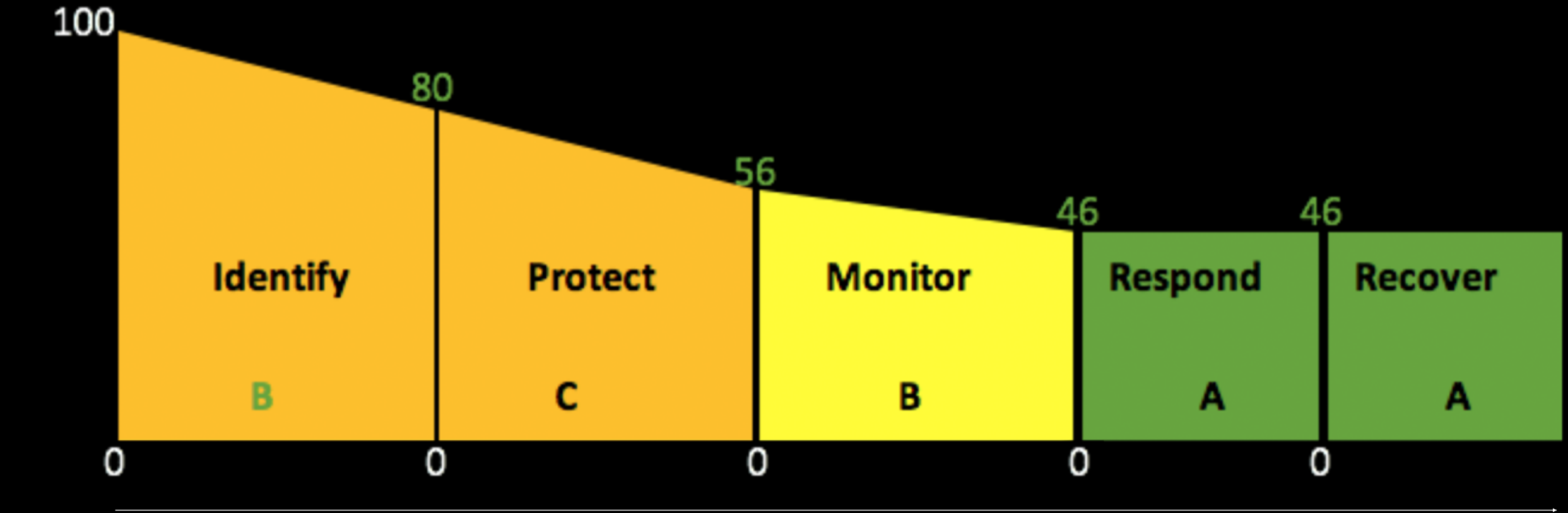
NIST Framework




Order of Operations Matter




Security Efficacy Answers




Strategy on a Napkin

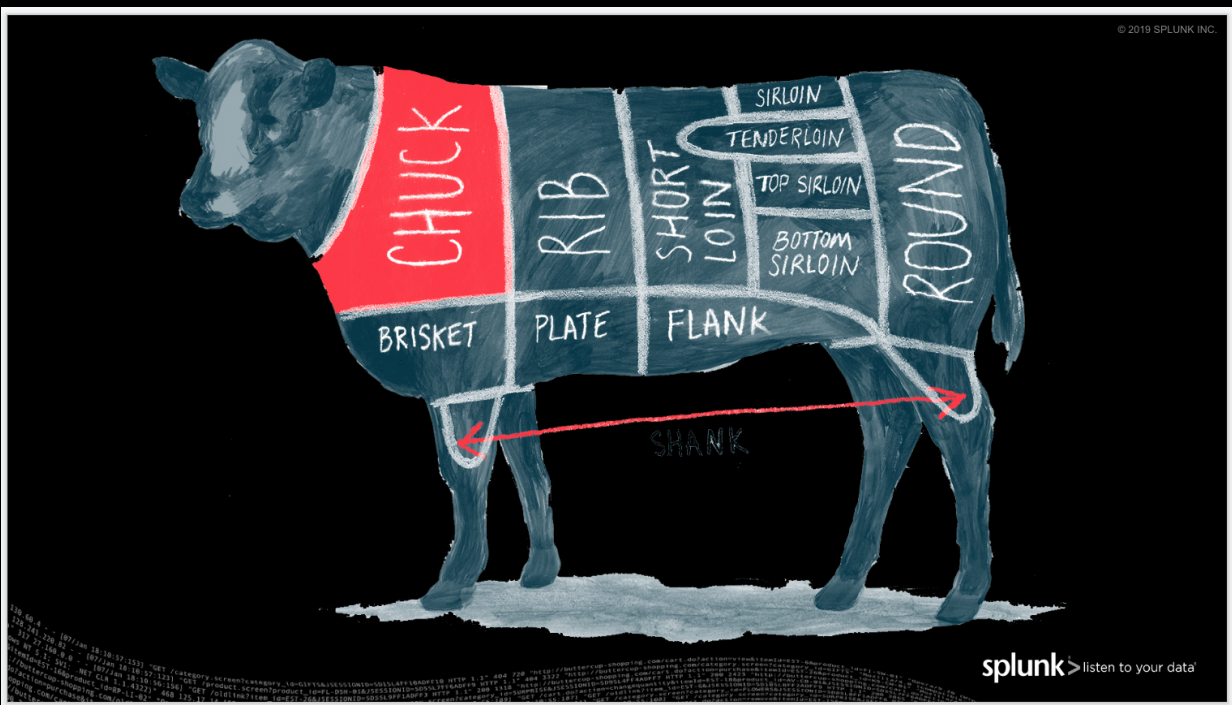
 Identify Protect Detect Respond Recover	Identify	Protect	Detect	Respond	Recover
Confidentiality					
Integrity					
Availability					

Strategy on a Napkin

	Identify	Protect	Detect	Respond	Recover
Confidentiality					
Integrity	X	X			
Availability	X	X			

Strategy on a Napkin

	Identify	Protect	Detect	Respond	Recover
Confidentiality	X				
Integrity	X		X →	X →	X
Availability	X		X →	X →	X



Thank you

Joel Fulton, PhD

CISO

jfulton@splunk.com

splunk >