In the Matter of:

Information Security and Financial Institutions Workshop

July 13, 2020
First Version

Condensed Transcript with Word Index

1

FEDERAL TRADE COMMISSION

INFORMATION SECURITY AND FINANCIAL INSTITUTIONS: FTC WORKSHOP TO EXAMINE SAFEGUARDS RULE

MONDAY, JULY 13, 2020
9:00 A.M.

VIRTUAL EVENT

2

FEDERAL TRADE COMMISSION

INDEX

	PAGE:
Welcome and Opening Remarks	3
The Costs and Benefits of Information Security Programs	23
Information Security Programs and Smaller Businesses	71
Continuous Monitoring, Penetration, and Vulnerability Testing	121
Accountability, Risk Management, and Governance of Information Security Programs	172
Encryption and Multifactor Authentication	222

3

WELCOME AND OPENING REMARKS

MR. LINCICUM: Good morning. I want to welcome everyone to the Information Security and Financial Institutions Workshop by the FTC. My name is David Linicum. I am an attorney here at the Division of Privacy and Identity Protection at the FTC. Today’s workshop is going to be looking at the Safeguards Rule, which is a rule that requires financial institutions to enact safeguards to protect customer information.

We’re going to start by looking at our current rule and what it requires of financial institutions and then move on to some of the proposed amendments that we issued. If -- and so, let’s go ahead and start the slides. Next slide, please.

Thank you. The Gramm-Leach-Bliley Act was enacted in 1999, and, among other things, it required several agencies to issue rules for financial institutions in order to have them safeguard their customer information.

In response to that, the Federal Trade Commission enacted its safeguard in 2002 and it became effective back in May of 2003. So over the next 17 years, no real changes -- well, no changes at all have been made to the rule. We think that shows how

4

flexible that rule has proven, and how robust. But we do periodically review our rules to see if there needs to be updates and we did so recently with the Safeguards Rule.

After that review, and seeking some comments from the public, we issued a notice of proposed rulemaking in March of 2019. We got quite a few comments back from proposed rulemaking, and this workshop is going to be looking at some of the issues raised both by the proposed amendments and by some of those comments. Next slide.

So let’s start with the current rule so we know where we’re starting from, what the amendments are -- would change and where they might expand upon the current rule. So the current rule applies to customer information held by financial institutions. Customer information is fairly self-explanatory. That’s information that a financial institution may hold that they received from a customer as part of providing a financial service or product.

“Financial institution” needs a little more explanation if you’re not familiar with it. I think most people when they hear “financial institution” think banks, and while banks are certainly financial institutions, they’re not covered by our rule. Our

have yet to be invented, we know. But if we’re doing an actual risk assessment, we’re looking at the likelihood and impacts of things that could go wrong in environments like ours. And what you’re also suggesting in the proposed updates is that there’s a -- that you also evaluate the controls, which is super important. If we’re going to have a good definition for rie

magnitude of the risk, you then have to look at a solution. In one way, the costs of those solutions are fairly obvious. You'll

that just can’t be applied.

We had a client, a hospital, that was -- they were fed up with their security team, their

cybersecurity model maturity certification. A new one

MR. MOLINA: So I noticed sadly we were doing a little bit of a hybrid online learning, hybrid remote work, until we moved to 100 percent remote. A number of things happened. You know, first we went to all Zoom sessions. And guess what? Then we got into Zoom bombing incidents because the bad guys realized, hey, this could be fun. And some of them were not fun. Some of them were even illegal and required collaboration with the FBI to report the culprits and everything else.

Then we realized that people working at home without peers on their side, multitasking, taking care

And adding those controls in has, I think, increased because of the pandemic response.

MR. LINCICUM: Great. We are just about out of time, but I wanted to ask one last question. And if you all could take about a minute answering a fairly big question, but, you know, as best you can.

We've talked about how information security is very particular for each company. It's going to have different needs. But are there some information security practices that are just so universal and so easy to implement that they should be just considered absolutely required if you were handling sensitive information like financial information?

MR. CRONIN: Go ahead, Pablo.

MR. MOLINA: Chris, after you, please.

MR. CRONIN: Okay. Because I’m probably going to say what you were saying because you’ve been saying these things, too. I’m going to take a step back and say let’s not talk about each control that should be expected because our risk analysis is going to show us how to apply those things differently, in different ways.

What I will say is you find the security control standard that looks like it addresses the risk that you've got in your organization and apply those

controls the best you can. And where they're difficult to apply, you do a risk analysis to see

I'd like to talk about the qualified individual requirement of the proposed Safeguards Rule. Several of you have mentioned the costs of the requirement in the proposed amendment to "designate a qualified individual responsible for overseeing and implementing your information security program." That is the language of the proposed amendment. This person may be employed by you, by an affiliate or by a service provider.

So the intention of that proposed language, as my colleague David Lincicum mentioned earlier, was to increase accountability and to lesson the possibility that there would be gaps in responsibility between individuals.

So, Brian, I'd like to ask you your opinion of the costs versus the benefits of hiring a "single qualified individual" to coordinate the information security program at a small business.

MR. MCMANAMON: Sure, Katherine. In TECH LOCK's experience, I think first and foremost it depends on what the definition is of a qualified individual. That individual would have to go through the proper security training in order to help lead and develop a security program within the organization.

In TECH LOCK's experience, most companies do

not have that qualified individual. And the reason for that is they're often -- they have a small IT staff; they're often wearing multiple hats. You know, you could be looking at an IT system administrator or an IT director or a CIO that's basically serving as that lead security person.

So what TECH LOCK has found that what works best is a combination of outsourcing to a managed services company. What that company can provide is that security skill set and expertise, especially in terms of potentially providing a virtual CISO role.

CISOs, as you heard, the average salary that's out there can range anywhere from 180K; it could be upwards of 400K. So providing that help and assistance on a strategic basis, I think, is what works best in transferring that knowledge internally. What a virtual CISO can help do is develop that security strategy and then help to implement that over time.

MS. MCCARRON: Lee, can I follow up with you then and ask what is the difference between what a qualified individual means for a smaller, less complex business? For example, can a small auto dealership have a less experienced person in charge of a program than a business with, say, a more complex network?

MR. WATERS: Definitely. If the dealership has any IT staff at all, they can take one of their more experienced people and they would have to do some research, maybe even call in a little bit of outside help, but somebody could definitely handle that.

With some of the smaller dealerships that only have, you know, maybe five people working the lot, they may not have anybody with IT experience. So they would have to go outside for help.

MS. MCCARRON: Thank you.

James, can I ask for your opinion as well? What do you see in terms of what a "single qualified individual" would mean in a small business versus a business with a larger, more complex network?

MR. CRIFASI: Sure. In the small financial institutions that we deal with, often the only IT staff onsite is maybe PC support or end-user support and there really is no IT management or upper level IT.

In those cases, we typically are working with the executive team. And what we found is that that executive team can really be the qualified person. Because at the end of the day if they have the proper advice and support or an MSSP or a virtual CISO, you know, that team is really who's going to

enforce everything and make sure that the business is adhering to the rules and the standards. Otherwise, it's just something that someone external has told them to do and no one really believes it or feels it or lives it.

So, in our experience, if we really involve it less as a find a single person and more as let's involve the head of finance, the head of business development, the head of operations and make that part of the team, it's a lot more effective for the smaller businesses.

MS. MCCARRON: M[illegible]

please, with Rocio. Wha

c خ s to s all businesses of re

outsource those qualified individual serv

You're on mute.

e now?

MS. BAEZA: All right. C

89

cover and the range of small businesses.

MS. MCCARRON: Okay, thank you.

Brian, a follow up question: How does the size of a financial institution and amount and nature of the information that they hold factor into an appropriate information security program?

MR. MCMANAMON: Yeah, I would agree that, you know, just to chime in on the last question, I think there are a minimum set of standards that need to be adhered to by small businesses. The way TECH LOCK views businesses and the way we scope the work that we do is based on number of users, number of endpoints, and then also number of sites and what their processing environment looks like.

So if you think about, you know, servers, workstations, laptops, the network footprint, any of those elements in an organization's environment may introduce a threat into that environment. So you have to look at that total threat landscape.

From a data prospective, you know, when we do audits on, for example, PCI or high trust, we follow that data, right, all the way from the -- where it comes into the environment and to how it's protected at each step, whether it's storage or processing all the way through to the back end. So

90

data does come into play in terms of size.

And if you were to compare, for example, to how PCI judges the size of an organization, you know, they do it based on level of transactions that a PCI data processor would process annually. So, you know, for example, over 6 million transactions, it would be designated that they would need to have an audit by an external auditor. Very small businesses would just have to go through what they call a self-assessment. But the issue that TECH LOCK has seen with those self-assessments, it's more of checking the box. Right? And that's what we're trying to avoid here. We want businesses to really go through that internal risk assessment and make sure that they are implementing the appropriate security controls for their environment.

MS. MCCARRON: Lee, I'd like to follow up with you about the issue of the size of a financial institution and the nature of the information that that financial institution holds, as a factor, into the appropriate data security program that they put into place.

Can you tell us from your experience whether it's the number of employees or the number of customers that you keep data about that's relevant to

91

to your business?

MR. WATERS: Well, I don't think the type of data really makes much difference as an attacker is just going to go for something easy that he's going to get a lot of information from. So the amount of data would definitely have an influence on whether a business is even going to be attacked or not.

The number of employees can also introduce other risks. The more employees you have, the greater you are at risk for either inside attacks or just social engineering. So you have to be prepared for pretty much everything from all sides.

MS. MCCARRON: James, how do you view the risks of how cybersecurity events change based on the size of a financial institution?

MR. CRIFASI: From our point of view, it's the point of view of the risk that changes, but we consider it pretty much equal risk. We have some small businesses we deal with that just have an enormous amount of consumer records, and so they might have a few number of employees or a few number of endpoints, but the amount of data available there is just quite vast. And so from that point of view, we would say, okay, they need to follow all of the safeguards, right? Because they just have such a

92

massive amount of data, they can't get away with just doing the basics.

On the flip side of that, we see small businesses where really they just need to focus on the basics. I know in Panel 1 they talked a lot about doing risk assessments and assessing what data is there, where it is and how it is. And there's a point of view for a small business that says if they get hacked at all, it doesn't matter if they lose employee data, financial data, consumer data, they're probably going to go out of business.

So there's a shift to me that says that when we look at a small business and we look at something like the safeguards, that doing the basics, or as Kiersten mentioned, changing the culture and making sure people are getting educated and understand security becomes more important, because really they can assume the level of risk, they can assume that at some point they will get an intrusion or malware or ransomware. An] Nr 12 φ , - tee

providers, making sure that they can develop and maintain safeguards. Well, there’s going to be very concrete questions. Do you have third-party data inventory? When was it last reviewed? When are you going to review it next?

And by having a different structure around the certification and also the annual report requirement, they can set up guardrails so that the organization is providing meaningful information. It’s very specific. And I think that that will be a more effective approach of raising organizational and CISO accountability.

MS. MCCARRON: Thank you very much.

I’d now like to turn to two of the requirements of the proposed Safeguards Rule that are specific to the technologies or the types of information security protocols that are put in place.

The first one is multifactor authentication. The proposed amendment would require financial institutions to implement multifactor authentication for any individual accessing customer information. Multifactor authentication, according to the proposed amendment, shall be utilized for any individual access in your internal networks that contain customer information unless your qualified individual or CISO

has approved in writing the use of a reasonably equivalent or more secure access control.

Brian, I’d like to ask you for your comments on this approach to requiring MFA for any individual accessing customer information in an internal network.

MR. MCMANAMON: Sure. Number one, you know, TECH LOCK fully supports this requirement. It is absolutely critical that organizations have multifactor authentication in place for accessing their systems or any of their applications.

To support that, TECH LOCK has implemented MFA for a number of our small/medium-sized business customers. The product that we normally use and we resell is Duo. So what I’ve done is pulled some pricing from Duo's website just to get an idea of what it would cost a SMB to implement.

As you can see there, there’s four different categories of cost all the way from free for up to 10 users to $3 per month. And what that adds is some additional security policy checks. $6 per user per month is the most recommended that has more robust device trust checks in place; more robust policy enforcement, and then all the way to $9 per use per month. That’s their premium subscription that has the most robust device trust checks. It also provides

application policy enforcements. And then you can implement single sign-on for some, their access to internal corporate resources.

MS. MCCARRON: Thank you very much for that information.

James, I’d like to ask you as well for your thoughts on the proposed amendments requirement that financial institutions shall use multifactor authentication.

MR. CRIFASI: Our point of view is we fully support multifactor as well. When we’re pulled into an environment that has had some kind of security incident or data loss or ACH wire transfer fraud, so far in the last, say, 12 to 18 months every single one would have been stopped by having basic multifactor authentication.

So from our point of view, it’s a good basic business practice at this point regardless of the Safeguard Rules or PCI or any other requirement. It’s just a good business practice to have, just to protect the internal information as much as it is to protect the company’s own internal information as much as it is to protect their consumer information.

I think the one thing that we see that becomes an issue is, you now, simply buying a

multifactor doesn't really give you a solution there because you have outsourced dealer management systems or loan management systems and you need to mab the multifactor will actually take care of all of the q! Q D A n ʊ ę l D T Mas well as remote a environment.

So I think flexibility there is really important. But at the same time, the definition really needs to encompass all of those nd of auxiliary and external @σviders, some of which we know from helping a lot of customers, they won't support it. You know, the dealer management system or associate management system, or core banking system, they won't support the multifactor.

And so we, as security technologists, we have to come up with an alternative method to secure that high-risk area. And it is available, it is possible, it’s things that can easily be done. Those service roviders don't always like it, but it’s a lot cheaper than, let’s say, telling a small business go change out the dealer management system that you’ve used for the last 20 years. The cost on that is going to be much more than that business can, you know, adapt to.

So I think multifactor is great, but we need to really consider those third parties and service providers in scope of that requirement.

MS. MCCARRON: A good point, thank you.

Now I'd like to turn to encryption, which is the other specific callout in the proposed Safeguards Rule -- amendment to the proposed Safeguards Rule.

The proposed amendment would require

MS. MCCARRON: Thank you very much.

Kiersten, may I have your concluding thoughts?

MS. TODT: Thank you. So I think some of the key points that are positive are focusing on things like multifactor authentication. I believe that right now multifactor authentication should be a default. And my hope for something like the Safeguard Rule that mandates multifactor is that it now starts to encourage those companies that can offer it and make it a default but don’t and leave it up to the user to choose to do MFA that you start to see incentives in the actual workspace and across industry for doing so. And I think that could be a very positive output from something like this.

The debate and the discussion we had on MFA

that are actually really cheap for this.

So for network monitoring, there's the Zeek network monitor. For monitoring end hosts, per se, you’ve got Syslog, Linux and Sysmon on Windows, and these both support remote log-in. You’ve got Nessus to inventory your network and know what's on it.

But to use those tools, you need experienced personnel. So you’ve got basically a tradeoff here. If you're outsourcing the work, you're spending a fortune. If you're insourcing the work, you aren't necessarily spending a fortune because if you're the

r

[redacted]

data. Financial aid data is really just a very small subset of what we do here at the institution. But it obviously, you know, could have major implications for us in terms of what we need to do to, you know, fund and staff a cybersecurity program.

So we need to make sure that as we’re thinking about what we need to cover in terms of the rule, we need to be very explicit about what that GLBA Safeguards Rule defines as customer information and how it fits in institution because arguably, when we’re doing a pen test, if I had called Scott and said, Scott, I want you to do a pen test but I only need you to pen test that financial aid data, but the reality of it is is that, you know, he could easily maybe get the financial aid data as, you know, Flee was talking about from somewhere else, you know, or I think Scott was talking about by going in a different way, from a different subsystem. Maybe it’s not my financial aid system; maybe it’s my admission system. Maybe it's something else that actually would provide that beacon that allows them to look in and see what’s there.

And so those kind of considerations are very important as we look at this information to make sure we're counting for it correctly.

MR. IGLESIAS: Great. Thanks, Tom.

Moving along to vulnerability testing, how often should an organization conduct vulnerability testing and what factors should they determine -- what factors should they consider in determining the frequency? Should testing be done, performed when there's been a change in the system or an intrusion attempt? Can it be automated and what does it cost?

And I would call to Flee to answer.

MR. LEE: Yes. So, you know, the TLDR here is that at a super, super high level, you can just think about vulnerability tey t w ʿ

_ st? ᵀ ʿ uv

L

9 Mook aor = ѫ я l l " Į ɞ ľ ʿ Ƃ

is how vulnerability scans actually work. So because they are doing some active things on the network, there could be network performance issues even inside of a, you know, test environment. There could be issues where a vulnerability scan could potentially impact those systems and the uptime itself. So that actually is something to watch out for, and part of the reason why it's good to actually have an expert on staff that can actually detect those nuances and also correct any errors that actually may be caused by the vuln scanning.

One of the other issues also to worry about with vulnerability scanning is, once again, kind of like this nature of scope, like how much of your ecosystem are you seeing and can you see. So in a really, really well segregated network, doing a vulnerability scan can be complex. You have to figure out where do you actually deploy the tools so you can actually see all of the network.

The other thing to actually also think about is how do you actually aggregate all that data. And, also, finally because of the nature of vulnerability scans, you also have to worry about this concept of false positives, meaning that you're going to find things that will show

Nick, are there any other products and services available to institutions for continuous monitoring and/or testing and what would these normally cost?

MR. WEAVER: There's a lot. And the cost is often a -- basically it’s a product of how much you're willing to spend and how much local expertise you have. So for network monitoring, you have free high quality network monitoring in the form of Zeek and Snort and Suricata and all those that are really good at logging everything that happens.

But if you're running them yourself, you’ve got to have an expert on staff, or you can go with one of the companies that’s outsourcing the skill. And so you don't need necessarily as much skill on staff, but now you have a big dollar line item. In terms of collecting on end host, it's the same thing. Sysmon is free; Corelight costs a fortune. But Sysmon means you have to have experts on staff who are able to set up a server to ingest the logs, to analyze the logs.

Similarly for log analysis, you can spend a fortune and go with Splunk, or you can go, these are logs I’m rarely going to read and so it's column/delimited text and you're using grep and Python, or you might be splitting the difference and

tossing it in the PostgreSQL database.

can actually help make that useful. You know, it's very sensitive as well.

MR. IGLESIAS: Great. We have another question that's asking, the Safeguards Rule is intended to set development of the comprehensive information security program in the context of what's appropriate to an organization size and type as well as nature and sensitivity of the data the organization handles.

With that in mind, how should the FTC work with different stakeholders, communities, covered by the rule to identify for organizations what the relevant standards for their industry may be in relation to these issues?

MR. LEE: I can chime in on that at a high level. I mean, there are tons of, you know, like essentially business organizations and representatives. I do think it's useful to distinguish between the size of these companies. What's appropriate and realistic from a security posture standpoint and security programs standpoint for a large financial institution, you know, such as Goldman Sachs or Bank of America, is very different than what it is for a 200-person company. And it's important that the FTC recognize that and really start to hyper-focus on particular behaviors that they want

to see and the outcomes of those behaviors.

And what that means is being open to examining the new guidance to determine if it's really, really truly outcome-based, meaning that not being overly prescriptive and saying that, hey, you have to have penetration testing, thinking more along the lines what you really want out of penetration testing.

The assumption is that you want penetration testing because you want to see businesses have ways that they can proactively find security weaknesses, and then once finding those security weaknesses, involved with and actually

one of the recommendations. Our CIO basically gave

So let me just start, Wendy, I'd like to ask you first. Starting with MFA, what is your view about whether IP address restrictions are a reasonable equivalent to MFA? Yes, go ahead.

MR. MARCHANY: Well, we would be the scapegoat. I mean, the moment there was a breach, then all the fingers would point to us and they’d say, hey, you said this was the way to work. And I said, no, what I said was the probability is, you know, much different. But, you know, you'd have to do other types of analysis. Maybe -- you were talking about, you know, behavioral analysis, looking at certain log-in times for certain user IDs. And you can sort of do that with sort of a continuous monitoring model. There's a lot of research going on in machine learning and AI in that type of area of behavioral characteristics. But, I mean, that is so far away from where I would go. I’m not sure I’d have an alternative plan to do that.

MS. MCCARRON: Okay.

Wendy, I’d like to ask you the same question. Could you provide us with your perspective on the possible burden to CISOs of having to write

265

risk, I believe, is ultimately a business one because mitigating that risk can cost money, effort, time. It can be an opportunity cost where the business is not moving forward on something else because they’re having to remediate something. And those sorts of decisions, including reputational risk, are not the sorts of things that the CISO can or should be making in my opinion.

MS. MCCARRON: Okay. Thank you.

So those are the rest of the questions from the audience. So I would like to wrap up by asking you all to just do a quick speed round, your lightning last thoughts on encryption and multifactor authentication that is in the proposed amendments to the Safeguards Rule. I would like to give everybody just about one minute to summarize or provide any additional thoughts. I’d like to start with Matthew, please.

MR. GREEN: Well, I mean, first of all, I think that we're in a great time when we’ve reached the point where we can actually mandate that encryption be used. I mean, years ago -- I’ve been in this field for 15, you know, 20 years now, I guess. And, you know, encryption used to be this exotic thing that was very, very difficult to use, very expensive

266

and not really feasible for securing information security systems. And we've reached the point where now it is something that’s come to be and we can actually build well. So I’m really happy about that.

And the same thing goes for MFA. We’ve reached the point now where we know that passwords do not work well. They are just simply not by themselves enough of an authentication feature. And fortunately there are a whole bunch of companies and inventors that come up with ways to make this better. And we're actually winning. I would say if you look at the overall progress of attackers versus defenders, the defenders -- when these systems are used and deployed, the defenders can win.

And now having those systems deployed is really the last final challenge. And I think that’s, you know, what’s great about these rules, is they start to make that happen. So that's it.

MS. MCCARRON: Thank you.

Randy, may I ask you for your final thoughts on encryption and multifactor authentication for today?

MR. MARCHANY: Yeah. I mean, certainly with encryption, as Matt said, it's become more commodicized, you know, now that it's not a big deal

267

from a financial standpoint.

As far as MFA goes, I always tell people, I say, look, when people push back, I said, you've been using two-factor for at least 15 years now. It's called an ATM card. And so when they -- when ct cry

A

a.m 1:13 61:14 70:6 70:6 120:15 148:6
abatement 152:11
ability

First Version

62:6 64:8 66:25
179:20 194:15
195:13 219:24
awesome 81:2 94:21
AWS 45:17

boards 194:13
body 14:11 96:2,21 97:4
bolstered 211:16
bombing 61:6
bones 11:21
bonus 36:10
book 46:17
bottom 244:22
bottom-tier 191:21
bottom-up 248:18
boundaries 53:23
bounties 130:17
bounty 130:22
box 73:23 90:11 134:8 268:7
boxes 134:17
brand 37:8 40:6
breach 14:2 15:22 25:20 27:21 28:7 31:18 33:25 34:11 51:6 53:24 54:3 93:10,13,17,23 97:24 143:6 154:12 159:22 206:9 219:19 235:25 236:1,2,3 236:15,24 249:2 251:4
breaches 98:5 118:8 122:25 143:2 197:22 245:22
breaching 52:9
break 21:12,17 69:24 120:12 220:25 252:8
breathe 212:16
Brian 71:15 77:15 80:18 83:22 89:3 102:3 114:5 115:11
Brief 22:15
briefly 172:18 215:18
bring 80:15 87:15 184:14 191:7 214:23 229:1 233:25 237:21 242:9
bringing 73:13 81:23 157:21 199:10
brings 20:14 113:24
broad 5:8 100:17 139:13 168:24 180:5 239:9
broader 128:25 174:23 175:17
brought 61:21 85:11 194:23 209:6
bubble 228:6
bucket 68:3
bucketed 117:22
bucks 236:14
budget 19:23 82:16 157:23 197:6
budgets 43:3
bug 130:17,22
bugs 237:8
build 29:23 76:22 115:22 154:14 188:16 194:15 205:25 219:2 266:4
building 128:21 150:19 188:24 189:10,11 191:3 191:14,15 197:16 211:25 212:23 216:14 245:15
builds 219:23
built 130:5 150:25 151:6 175:24 189:1 215:11 230:7 258:13 259:8
built-in 258:14
bulk 155:25 156:2
bunch 35:20 47:8 136:3 144:3 266:9
bundled 233:1
burden 60:15,22 85:20 96:19 140:15 248:23 249:19 250:17
burdensome 51:19
99:14 100:11 169:22
burner 246:16
business 8:7 14:6 15:25 21:2 27:9,13 28:18 29:8,17 30:6 30:11 32:10 35:11 38:24 39:9,15 41:2 42:16 44:19 50:6 54:10 56:16,17 62:9,16 63:16,24 73:5 74:20,22 75:11,13,19 77:18 78:23,25 79:13,14 80:1,8,19 81:9
2 82:14 84:9,12 85:10 :18 10,22
85:17 86:16 87:2,4 87:9,21,22 91:1,7 92:8,11,13 93:7,21 93:24 94:3 95:23
102:12 103:18,20
85:20 89 20 89 13
104:20,23 110:10 110:20 112:19
2 114:13,17 120:6 14
129:7 135:13,21 136:9,21 153:23 161:16 169:2 170:7,10 180:18 180:18,19,23 181:2,5,12,13 182:17 186:22
187:10 189:5,8
25 :14 18 2:33 13
198:18 200:10 203:9 204:19
2910 3 :2
216 12 1 0:14 17
251 142:92

258:8 270:7
cases 79:20 123:25 127:2 143:23 152:1 188:18 211:17 225:12 226:24 232:16 240:6 241:8 244:11 252:19 256:13 267:20
catalyst 98:8
catch 131:7
catch-all 8:11
categories 102:18
categorization

253:21 258:3

covered 4:25 10:5 58:24,25 67:21 137:20 161:10 227:10
covers 5:2 8:16 228:25
COVID 44:21 145:22 152:12
COVID-19 59:17,23 60:1
CPA 233:15
crack 133:13
cracks 183:10
crafted 263:5
crazy 49:8 132:8 226:18,22
create 8:25 110:18 111:3 114:19 202:1 217:10 218:3,5 248:16
creates 33:9 88:3
creating 15:10 49:21,21 95:11 96:23 97:12 110:24 111:7 218:20
creation 9:10
creative 126:6
credentials 67:2 132:10,11 134:7
credit 9:3,3 228:21 236:11,16,18
creds 134:18
Crifasi 71:13 72:15 72:19 74:16 79:15 91:16 103:10 107:18 113:1
crime 154:9
crisis 252:15
criteria 11:18 191:22
critical 43:12 61:20 61:21 94:5 95:15 97:5 99:1 102:8 107:12 115:3 143:11 147:18 155:8 167:5 168:1 174:9 192:3 199:3 202:16 205:19
Cronin 23:17 24:6 26:25 39:17 48:10 50:23 54:21 56:13 60:25 62:11 65:14 65:16 70:4
cross 26:2
crunch 59:24
crunchy 132:21
Crypsis 23:19 28:6
crypto 132:12
cryptographer 222:20
cryptographic 239:21
cryptography 222:22,23 223:1
CTO 23:15 71:13
CTO's 145:10
cubicles 76:22
culprits 61:9
culture 87:14 88:8 92:15 97:12 98:3 111:3,7 113:25 195:4 210:23,24 211:2
cumbersome 160:20
curious 200:23 227:11
current 3:12 4:12,15 4:15 6:7 8:14,15 8:18 9:9 10:17 11:3 12:6 13:7,16 13:23 23:23 29:22 30:3 73:13 74:10 74:10 142:1 173:3 176:21 181:16 193:16 200:19 204:25 237:19 255:14
currently 53:8 72:24 81:14 139:24 253:5
curtail 37:6
curve 214:12
cusp 144:20
custodianship 166:19
custom 142:5,5
customer 3:10,20 4:16,17,19 5:17 6:15 7:1,3,20 10:8 17:2,15,20 18:9,10 20:12 55:22 85:25 86:12 101:21,24 102:5 105:9,12,15 122:4 137:21 138:9 148:2 160:11 189:1 199:2,18 224:3,8 230:19 256:20
customers 5:12,13 5:18,19,23 14:6 19:23 84:10 86:1 86:11,14 90:25 102:13 104:11 176:20 188:18 220:13,14 232:3 243:5
cut 36:16 254:11
cyber 9:5 14:1 38:17 47:14 71:19 86:21 87:21 92:22 93:13 98:17 108:1 143:2 146:22 147:16
cyber- 111:16
cybercrime 43:24
cybersecurity 23:19 31:4 35:15 37:13 37:17 38:14 43:19 44:11 46:16,17 47:9 48:8 49:25 57:1 66:10 75:25 76:3,15 86:23 91:14 93:2 94:4,12 94:18 97:6 110:11 111:6 115:7 119:11 132:20 138:5 ة Ǿ **5 η**
1 Ƭ Ô ₵ cusn Cr ḱ 53:8 Á
24 þ 93:

79:6
dealing 192:23 218:8 244:9 253:19
dealt 76:15
debate 117:16
debt 5:10 144:1
debugging 125:16
decade-old 155:22
decent 168:6
decide 17:11 150:5 200:4 207:12,13 229:6 232:21
decided 19:20
deciding 204:2 207:1 216:6
decision 19:16 184:8 190:1 200:5 201:22,23 202:8 204:18,23,24 206:2 208:20 216:3 225:22 232:20,23 235:17 250:8 264:25
decision-maker 189:24
decision-making 173:25 175:9 182:22 184:21 187:6

169:4,12
EternalBlue 135:2
Europe 54:14 132:14,15
evaluate 8:2 13:22 25:6,10 34:2
evaluating 27:15 192:12
evaluation 15:12 24:21 25:8 41:24 51:14
event 1:16 14:1 93:17 94:1
events 15:19 91:14 93:2 94:12 96:10 116:23 122:1
eventually 214:13
everybody 57:25 60:21 64:1 111:3 113:11 114:1 157:16 170:3,8,25 213:23 228:14 236:20 244:2 264:18 265:15
everybody's 98:3
everything's 32:7 45:16
evidence 40:20 206:9,10
evidencing 203:11
evolution 98:17
evolve 98:19
evolves 261:17
evolving 30:1 111:16
exact 13:15 259:9
exactly 9:14 10:3 15:14 16:21 17:9 39:18 169:19 233:8 252:10
EXAMINE 1:5
examining 162:3
example 28:16 37:7 37:12 47:15,17 52:1 55:25 56:20 60:16 73:10 74:10 78:23 81:23 82:23 89:21 90:2,6 106:3 107:21 108:2 112:6 113:9 123:5 123:9 124:2 130:5 133:1,22 137:23 142:6 150:23,25 155:20,25 163:24 164:4 182:14,18 190:17 200:14,18 200:18 203:13 216:1 218:8 219:20 225:3 229:15 233:3,10 233:12 240:2,20 241:9,21 242:6
examples 100:16 202:11 203:13,17
excellent 186:6 268:16
exception 10:6 19:19 51:1,13,14 56:10 202:21,23 203:2 250:18
exchange 111:15
exchanging 111:11
excited 26:5
excluded 5:5
execute 246:23
executive 36:18 79:21,22 97:4,21 97:21 98:15 189:20
executives 57:5 263:22
exempt 20:8 85:22
exempted 86:14
exemption 88:13
exemptions 85:24
exempts 10:8
exercise 31:1 142:16 208:21
exfiltrated 262:11
exfiltrates 32:11
exfiltration 261:19
existing 73:1 74:7 74:14 75:19 76:22 81:20 197:4,5
exists 38:17
exonerated 88:24
exotic 265:24
expand 4:14
expansive 163:16
expect 81:21 83:19 95:1
expectation 100:25 115:16 162:15 252:21
expectations 99:18 112:5 116:2
expected 65:20 122:15
expecting 81:15 107:11
expense 123:11 151:19
expensive 43:10 74:1,2 123:12 124:5 129:19 130:7 157:15 250:11 255:25 256:19 265:25
experience 11:15 20:16 30:18 31:20 37:11 38:4 73:11 77:20,25 79:8 80:6 90:23 223:5 242:24 250:19
experienced 33:25 75:6 78:24 79:3 125:7 187:16
experiences 172:19
experiment 198:11
experimenting 196:22
expert 141:8 149:13 212:10
expertise 20:19 78:10 120:11 130:7 136:25 144:10,21,23 149:7 150:6 156:10 157:5,14 158:4 233:14 247:7 258:9 268:12
experts 20:18 31:10 68:23 71:5 120:3 125:23 136:11 149:19 158:6,7,7 222:8
explain 36:7 38:17 47:7 108:17
explanation 4:22
explicit 11:4 51:15 138:8
explicitly 27:5 128:4
exploit 126:20 134:1
exploitable 132:7 142:2 143:24
exploited 127:5
exploiting 129:5
exploits 127:10
expose 55:3 57:15 262:11
exposed 54:2 236:12
exposure 32:13
extended 203:3
extends 189:23
extent 105:11 129:22 181:24 182:11 190:11 253:2
external 6:25 17:18 17:24 76:16 80:3 82:12 90:8 104:10 105:10,13 131:16 131:21 132:3,7,10 132:19 147:1 148:21,23 150:6 151:4 189:4 208:13 210:18 213:8 215:5 224:4 224:10
externally 129:20 131:19
extra 76:21 193:9
extraordinarily 140:3
extremely 184:25 185:5,15 225:4
eye 124:9,13 185:3 185:14
eyes 28:10

F

face 19:9 28:1 31:17 191:17
facilities 125:15
facing 28:15,18 29:1 31:13 69:6 252:25
fact 87:9 113:2 119:22 123:7 137:18 139:24 143:3 150:13 151:22,25 152:9 152:16 155:9,11 168:9 179:21 208:20 213:25 226:13 235:3 244:14 245:8,20 245:25 248:10 252:6
factor 18:19,23 19:4 19:5 49:10,13 61:23,24 89:5 90:20 94:15 95:15 207:18,23,24 208:6,16,23 230:22,24,24 231:2,2,7,11,14 243:14 245:7
factors 18:18 126:12 139:4,5 190:14 196:19 215:6 230:21 233:22 234:3,9,11 242:5
faculty 30:7 37:16 121:11 237:4
fail 93:12 242:2
failed 49:18
fails 87:3
failure 36:17 170:13
fairly 4:17 5:7 33:3 53:1 65:6 69:17 130:4 168:24 178:1 190:5
fall 30:22 58:22 183:7,10 232:5 239:7
falling 43:22 74:8 235:1
false 141:24
familiar 4:22 18:13

38:7 187:18 201:9
familiarity 196:6,7
Family 56:21
famous 245:22
fan 105:22 115:20 116:11
far 24:4 31:18 103:14 111:10 232:6 248:21 249:13 267:2
farm 132:15
farther 205:2 259:19
fashion 15:9 16:2 18:14 163:3
fast 116:14 199:25
faster 182:21
favor 235:1
favorite 115:15 132:9
FBI 61:9
feasible 18:3 94:24 226:3 266:1
feature 218:25 219:3 230:10 243:8,10 266:8
features 128:21 228:17
fed 49:3
federal 1:1 2:1 3:21 24:19 25:18 36:23 39:25 56:24 63:13 71:25 97:24 173:13 222:6 234:8 235:7 243:4
feedback 71:19 85:16 199:11,21 200:12
feel 20:4 122:11 165:10 176:20 217:4 222:15 247:21
feels 80:4 85:6
felt 16:25 59:25
FERPA 56:21 57:14
fewer 86:1
field 12:4 20:18 42:7 44:17 48:4 265:23
fields 38:6
fifth 174:17 222:3
figure 41:15 42:17 54:23 72:23 136:20 137:10 141:17 147:5 154:19 186:16 219:20 248:15
figured 42:9 151:21
figures 85:13 129:17 129:25
figuring 136:13 214:5
file 49:12 155:2 229:8,20 260:13 260:14,16,20 268:22
files 259:3 260:19 261:5,5
fill 210:1 211:11
filled 80:16
filter 39:8
final 112:16 170:17 221:1 222:3 229:9 237:8 266:16,20
finalized 83:20
finally 6:14 8:11 10:6 21:19 71:20 84:15 141:22 162:13 223:8 224:12 233:20 267:8
finance 74:24 80:8 173:18
financial 1:4 3:4,9 3:12,18 4:16,18,20 4:21,23,24 5:2,3,7 5:15,17,19,21,22 5:25 6:8,9,10 7:5 7:13,19,21 8:1,6,9 8:23 9:1,13,15,20 10:13 12:16 13:5 13:13 16:20,23 17:1,2,6,10,21,23 17:25 19:21 20:17 23:22 28:18 36:23 36:25 37:3,10,23 39:23 41:25 43:6 48:6 55:23 56:1,22 57:12 65:13 72:11 74:7,12 79:15 80:14 85:20,24 86:1,11,13 88:14 89:4 90:18,20 91:15 92:10 93:3 94:13,15,19 95:14 96:1,5,13,16,22 101:19 103:8 105:8,11,14 111:22 137:25 138:1,13,15,19 153:19 160:12 161:21 163:25 170:7,12 176:2,9 181:17 182:1,13 182:14 186:25 194:1 198:22 199:1 200:5,16,19 201:8,10 209:11 209:17 223:20 224:13,21 226:8 226:19 228:3 229:12 230:17 232:1,19 233:21 234:7 235:16,24 236:20 237:14,15 237:17 238:23 240:12,16 242:20 242:25 243:13,16 244:16 247:24 249:23 256:16 264:15,17 267:1
financially 270:10
find 8:4 31:12 41:5 63:8 65:23 80:7 113:13,20 120:7 128:2 130:14 131:7 133:6 134:2 136:16 141:24 143:16 144:6 145:11,16,25 154:18 158:19 160:21 162:11 163:1 164:24,25 167:17,17 168:17 187:16,20 206:9 206:10 228:10 229:2,6
finding 126:23 162:12 268:3
fine 137:6
fine- 58:5
fine-grained 58:1
fine-tune 58:2
fines 37:10
fingerprinting 247:4
fingerprints 19:7 54:5 231:4
fingers 249:3
finish 21:20 25:25 26:2 52:24 164:17 166:22
fintech 81:10 94:21 183:15
fintechs 83:4 112:3 116:13 182:18
firewall 43:11 45:2 60:14 74:2 84:25
firewalls 67:2 144:1
firm 23:19 28:6 188:20 197:13 213:6 233:15 258:15
firms 28:13,14 241:9,10
first 6:7 7:22 10:13 17:15 21:24 22:13 23:4,12 27:2 61:4 72:5 77:20 81:2,5 81:19 87:1 99:17 101:18 111:6 131:21 137:24 172:25 173:23 177:1 181:24 182:8,11 183:23 187:1 190:19 194:2 198:10 201:8,14 202:12 202:19 204:16 222:19 224:1,7,18 224:23 229:6 230:21 231:9,22 244:8,8 245:2 251:8,10,16,20 252:14 259:25 265:19
fit 50:9 82:9 83:14 137:19
fits 127:14 138:10
five 24:13,17 40:11 40:11 41:5 71:4,7 79:7 81:16 109:16 156:1 257:20,21 257:21
fix 127:7 129:4 144:12 163:3 199:19 202:23
fixed 136:17 168:23 202:25
Flee 121:13 126:14 129:6 130:24 135:6 137:12,15 138:15 139:9 142:21 143:1 158:18 168:3 170:1
flesh 11:21
flexibility 8:18 98:19 104:7 203:12,19 213:9 223:23 237:20 255:15 267:23
flexible 4:1 8:16 88:25 114:20 257:7 267:19
flip 92:3 238:4
floor 76:23
flow 116:4
flows 166:10
fob 244:10
fobs 239:12
focal 67:19
focus 45:9 87:11,14 88:8,21 92:4 94:5 119:6 163:1 184:15 192:17 222:23
focused 83:7
focuses 87:19
focusing 86:24 93:25 117:5

folders 229:3
folks 74:23 108:17 132:25 213:3
follow 66:12 74:5 78:20 88:3 89:3,22 90:17 91:24 206:3
followed 206:15
following 22:6 62:9 96:3 160:17 190:18 196:19 218:17
followup 99:2 184:23 202:24 226:5 227:22 229:9 232:18 253:12 257:10
food 62:1
fool 248:8
footprint 89:16
forbid 183:21
force 236:23 241:12
forced 88:2
forcing 40:25
foregoing 270:4
foreign 256:9
foremost 77:20
forensic 58:10
forensics 157:7
foreseeable 6:24
forever 144:14
forgotten 62:8
form 40:5 134:22 149:9 173:22 201:10 226:19,20 228:16
formal 208:13
formalized 203:8,22 203:24
format 160:16
former 250:14
forming 190:1
formulate 195:24
forth 9:18 20:22 53:14 107:6,7 159:12
fortunately 266:8
fortune 125:10,11 149:18,22 153:21
forums 66:15
forward 26:9 40:2 172:15 173:9 174:11 181:6,14 207:1 258:3 265:4
fosters 200:25
found 75:10 78:7 79:21 113:12 185:5
foundation 115:17
foundational 115:21 116:9
founding 23:16
four 23:7 24:13 40:11 102:17 108:11 146:10 234:5
frame 159:10 180:24
framework 49:24 49:25 173:17 177:3 197:4,24,25 205:18
frameworks 47:21 50:13 174:2 196:24
framing 180:23
Franchise 72:10
frank 63:23
frankly 182:25 201:19
fraud 28:20 103:13 240:5
Fredrick 121:12
free 102:18 122:11 140:4 144:6 148:8 149:8,18 151:11 217:4 222:15 225:18 233:12,13 233:17
freely 41:23
frequency 126:13 139:6 140:7
frequently 26:14 140:19,24 142:13 227:24
friendly 240:1
friends 53:22
front 185:1 208:19 232:14
fronts 173:23
fruition 196:18
frustrating 62:23
FTC 1:5 3:4,7 23:4 23:6 42:11 46:15 46:18 48:22 50:3 52:13 53:22 54:12 57:13 66:16 68:16 121:5 137:24 156:12 161:9,24 167:1 168:8 169:10 172:4,8 206:25
FTC's 121:4 181:16
fulfill 116:15 209:12
full 7:11 32:3 146:17
fully 102:7 103:10 181:13 188:15
fun 61:7,8
function 95:4 213:23
functionality 228:24
functionally 250:4 250:21
fund 138:4 250:10 250:10
fundamental 68:18 168:16 195:9
fundamentally 9:10
fundamentals 50:17 69:12
funding 57:3 199:15
funds 176:11
funnel 99:25
funny 56:13
future 30:3 162:19 206:17,19
future-looking 174:6

G

gaining 196:23
gaming 145:10,16
gamut 126:18 129:21
gap 45:8
gaps 33:20 77:13 82:1
garbage 133:24
Garseki 158:3
gather 20:20 151:10 154:21
gathering 154:11
GDPR 54:13,20
gears 181:15
general 27:25 38:5 66:11,23 125:17 129:15 147:25 179:20 192:15 217:20 218:16 235:1 239:8
generally 5:6 10:22 24:9 38:7 129:18 132:1,6,16 134:21 159:10 179:4 200:15 207:5,15 207:21,22
generals 54:13
generic 100:15,17
geographical 257:25
geolocation 245:13 246:4
George 270:3,16
Georgetown 23:14 32:18
gesture 23:10
getting 28:19 36:10 40:1 48:23 52:9 61:25 62:23 92:16 98:13 109:4 119:8 129:22 148:18 155:10 164:17 166:14 181:6 208:12 213:10
gift 61:16
gigabyte 124:4
give 5:20 9:3 10:24 11:20 14:22 67:23 104:1 107:25 119:19 127:6,25 135:11 147:4 148:17 152:24 164:21 166:13 212:18 217:20 218:5,8,9 220:8 253:8 255:15 264:5 265:15 267:13
given 34:2 51:19 53:7 188:7 198:25 202:14 210:2
gives 10:3 18:25 55:25 131:3 145:8 235:9 236:15
giving 69:22 253:10
glad 174:14
GLB 71:3 72:6,12 75:19,22 121:4,20 160:9 222:3 259:19 268:14
GLBA 138:8 163:13 237:15
global 87:5
Gmail 228:4 254:18 255:11
go 3:14 6:5 10:4,11 12:22 14:19 17:9 18:11 22:8 23:8 24:15 25:3 29:19 37:19 40:9 41:5 44:2 45:24 46:17 55:9 60:25 65:14 75:12 76:9 77:22 79:9 81:5 87:12 90:9,13 91:4 92:11 104:20 109:15 110:12 112:16 113:13 124:19,22 126:12,17 129:25 131:5 146:14 147:4,13 149:13 149:22,22 157:6 157:10 158:23 164:3,4,14 167:1 174:13 178:25 182:8 188:10 194:2 196:9 199:18 201:24 202:7,23 204:4 207:14,18 208:25 214:3 215:18 218:24 220:2

245:17
happening 24:18 62:15 63:1,25 150:4,4 159:6 182:12 189:6
happens 6:23 20:1 33:16 59:2 149:11 193:12 206:12 208:24 213:24 215:9 228:1 236:3
happy 41:4 42:7 157:17 174:10 182:10 264:19 266:4
hard 27:17 36:3,7 36:12 39:10 41:15 50:9,9 54:23,24 68:5 132:21 143:15 144:18 150:21 151:10 154:18 158:25 183:8,8 185:10 187:11 189:4 193:3 196:17 211:3 233:4 255:16 264:24
hard-pressed 164:15
hardcore 43:21
harder 59:25 182:24
hardware 235:6 239:17
harm 14:5,5 24:22 26:25 27:5,7 53:4 53:10,19,24 54:1,6 54:8,8,16 55:2,6,7 55:10
harmed 25:13
harmonizing 112:1 112:10
Hartley 162:21
hash 205:3
hashes 133:4,7,8,12 133:13
hashing 134:25
hasn't 26:7 219:22
hat 81:21 82:6,11 178:3 183:12
hats 78:3
haven't 26:20 33:25 38:19 42:9 94:23 151:20 217:2
haystack 145:16
he's 91:4
head 80:8,8,9 172:13 178:2,3 180:25 187:7,13 187:20 191:23 223:9
heads 263:6
health 255:5 262:21
healthcare 234:6,22 241:21 242:6 262:19
healthier 49:17
hear 4:23 24:15 47:11 51:6 80:25 168:4 186:21,22 201:24 217:11 234:19
heard 30:20,22 78:12 84:2 114:14 152:18 202:1 259:15
Hearing 269:3
heart 54:11
heat 178:24
heavily 240:18
heavy-handed 203:9
held 4:16 17:16 56:2 88:19 105:9 224:3
help 35:16,18,23 41:17 42:22 44:25 67:5 68:23 75:24 77:23 78:14,17,18 79:5,9 81:24 84:6 88:21 109:23 118:2 127:5 129:2 140:4 145:25 151:17 157:1 181:5 187:21 199:13 220:17,24 243:15 249:22,22 258:25
helped 72:20
helpful 47:14 55:15 68:13 185:6 198:12 201:16 205:9 210:1 211:17
helping 5:12,13 28:8 69:20 86:23 94:6 104:11 110:21 180:19 199:23
helps 41:23 46:21 50:22 201:21 202:20
here's 27:18 29:6 45:17 46:17 59:15 197:2,5 217:1
hereto 270:9
hey 35:9 36:7 38:25 46:17 61:7 67:9 128:1 133:2 136:4 162:5 196:10 244:2 247:15 249:4
Hi 222:2
hidden 108:13 234:12 236:10
hide 107:24 143:21
hiding 45:3
high 43:5 89:21 99:23,24 118:18 118:24 132:2 139:11 149:8 151:19 161:14 17 ž igh ă
2025:4 110:211

2025. 252
201:. /0

hf 38- 1532559 : 13& n

236 Þ 1 } ž ŋ 4̈ Ǝ ϰ 75:24 :12
51:6 5 9:6 Ʈ

5 þ

6 ß ž ǿ 461m ȿ
1782,5 21 hc

/000Ŵ Ů l p ę ᵀ
20 69 ¿ ž
14 ˁ

independently 153:1
indicated 34:15 174:15
indicators 35:22 94:17
indistinguishable 160:2
individual 10:14 18:9 74:15,19,23 75:4 77:2,5,17,22 77:22 78:1,22 79:13 80:23 81:21 95:25 97:7,9,18 101:21,23,25 102:4 105:17 109:22 110:4,12 113:10 119:9,13 119:16 163:7 201:23 230:18
individually 233:7
individuals 30:16 42:3 77:14 81:19 111:1 193:24
industries 48:1 50:15
industry 38:22 48:6 48:13 50:17 51:3 94:23 117:13 130:19 161:12 164:6 196:23 199:1 233:25 234:6 244:2
industry- 36:21
industry-adjusted 48:11
industry-sensitive 47:16
industry-specific 112:5
ineffective 47:1
inexpensive 224:20 226:7
infeasible 105:14 224:14
infected 62:23
influence 91:6 184:20 219:8 241:5 253:7
influential 184:19
info 160:11
information 1:4 2:6 2:9,16 3:3,10,20 4:16,17,18 5:17,19 5:20,21,25 6:3,6 6:13,15,17,18 7:1 7:3,9,11,20 8:2,10 8:13,20 9:11,16,24 10:8 11:6 12:3,25 14:12,15,21,23,24 15:18,24 16:14,15 16:19 17:2,16,20 17:20,24 18:6,9,11 18:21 19:21,24,25 20:3,7,13,16,19,21 20:24 21:11,13,19 23:1,13,21 24:20 24:24 25:21 27:24 28:2,12 30:13 31:17,21,24 32:1,9 35:19 36:14 39:22 40:25 43:4,17 45:19,20 47:20 48:12 53:20 55:22 55:22 56:1,4,8,20 57:12,15 62:14 64:21 65:7,9,13,13 66:13 68:19 69:2 69:25 71:1,5 72:4 76:2,25 77:6,17 80:19 85:25 86:12 89:5,6 90:19 91:5 96:3,4,6,12,16,22 99:25 101:9,17,21 101:25 102:5 103:5,21,22,23 105:9,12,15,24 108:20 111:15 115:17,23 121:11 121:13,24 122:4 124:22 125:12 126:10 137:19,22 138:9,24 143:5 154:19 160:10,23 161:5 162:15 172:2,12,20 173:12,15 174:6 174:24 175:2,6,10 177:10,12,14 178:17 179:2,6,10 181:18 182:23,25 185:1 188:3 192:16,25 193:25 194:6,14 210:14 210:22 215:22 218:4 219:1 222:21,25 224:3,8 224:9 230:19,23 238:21 247:19 255:8,12 259:20 261:19 266:1
informative 171:2 230:12 235:14 268:13
informed 96:21 173:25 181:13 184:8
infosec 28:14 36:18
infrastructure 131:5,6 160:5 227:15 238:23 251:11 253:4 260:9
ingest 149:20
ingestion 123:24 124:3
ingredients 25:22
inherence 19:5 231:2
initial 88:5 134:10 147:8
initiated 254:12
initiatives 174:6
inject 51:20
innovating 40:12,18
innovative 167:17
inordinate 57:24
input 198:3 220:24
insecure 33:18 128:4
inside 59:4 60:8 91:10 132:22 141:3 159:23 210:6,16 212:19 226:25 239:18 242:14 245:14 246:1
insider 191:10
insight 135:11 214:16 215:5 256:5
insourcing 125:10
Ḉ

257:15 2 ˇ 128:49q,13, þ Ɣ 66:19 266:1

First Version

First Version

217:21
layers 204:15,17
lays 6:1 11:17 12:20 13:25 231:5
lead 77:23 78:6 106:24 109:25 175:24 179:1 185:24
leader 111:13
leadership 33:13 35:24 64:8 97:3 98:13 111:12 175:5 179:4,12 180:1,15 184:9 185:21,22 194:7 195:5,17,19,23
leads 207:24
learn 137:11
learned 62:8 256:10
learning 61:2 216:16 249:11
leased 255:20,23 256:3,22 257:4,6,9
leave 116:19 117:11 215:8 237:20 260:15 261:5 263:6
leaves 48:15
leaving 174:20 239:10
lecturer 23:14 121:17
led 223:10
Lee 71:20 75:16,17 75:20 76:24 78:20 90:17 119:19 121:12 126:15 129:9 135:8 139:10 156:5 161:14 165:8 168:4
leeway 166:12
left 72:3 109:12 216:24 218:23
legacy 45:2 60:6
legal 31:9 111:23 148:16 206:18 216:5 218:16
legitimate 15:25
legs 160:12
lender 95:1
lenders 5:10,10
lending 81:11 107:1
lengthy 53:1 55:18
lens 95:22 130:13
lessen 14:5
lesser 253:2
lesson 77:12
let's 99:17 186:10 188:14 206:8,15 225:17
let’s 3:14 4:12 6:5 10:11 17:14 24:2 55:25 57:20 59:19 59:20 65:19 80:7 100:17 104:20
letters 37:9
level 28:25 41:3 43:20 55:6,12 60:11 64:8 73:2,13 75:5 79:18 83:9 90:4 92:18 97:23 100:4 118:19 133:22 139:11 144:23 161:15 179:12,22 180:5 194:7,17 195:10 203:21 205:16 209:4 211:8 219:24 241:4 250:8,9,16 262:19 263:22 264:13,17 264:17
levels 43:1 108:11 178:20 180:2
leverage 45:13 50:18 95:6 166:13
liability 116:20 218:20
liberal 163:19
license 228:21 229:18
licenses 230:6 233:12 257:18
licensing 229:17 233:1
lies 8:15 187:6
life 18:15 62:24,25 176:1
light 170:9 201:18
lightning 218:23 265:12
likelihood 24:22 25:3 34:22 51:16
likelihoods 25:9
likewise 198:10
limit 14:21 260:20 260:22 261:6
limitations 116:21 131:11 153:11 253:18
limited 52:15 110:22 145:19
limiting 64:21
Lincicum 3:2 23:3,5 27:18 32:21 38:2 45:24 47:11 52:22 55:17 59:14 65:3 69:14 77:11
line 25:25 26:2 31:12 35:11 149:16 177:1 183:4 187:2 190:19,21,22 233:19 240:17 244:22 256:22
lines 44:18 59:11,11 109:24 158:18 162:7 190:9,18 255:20,23 256:3 257:4,6,9
lingering 43:14
Linicum 3:5
link 22:3 30:23,25
links 179:18
Linux 125:4 142:6
list 75:4 131:17,25
listen 186:14
listening 222:14 268:16
literally 128:6
litigation 27:1
litigators 24:20
little 4:21 10:7,12 11:20 12:7 16:22 19:9,18 20:10 35:4 44:24 61:2 66:11 68:14 73:6 79:4 114:3 123:6 126:21 130:18 132:18 159:7,10 163:12 168:10 170:4 175:12,23 178:14 191:5,6 195:11 203:10 207:6 219:23 226:22 239:12,25 243:9 252:8 253:10
live 110:14 123:15 164:14 205:1 212:16
lives 80:5 194:24
LMS 95:2
loan 95:2 104:3
loans 5:12,13
local 45:4 76:14 149:7 230:3
located 15:2
location 152:2 246:18
LOCK 71:16 78:7 84:2,9,18 85:6 89:11 90:10 102:7 102:11
LOCK's 77:25
LOCK’s 77:20
locked 242:12
log 122:21 149:21 233:9 234:16 240:23 244:12
log- 249:8
log-in 85:1 125:5
logged 132:11 134:8 134:15,17 155:16
logging 122:21 124:21 125:15 131:5 149:11 153:14,17 154:2,4 154:10 155:21 156:7 158:14
logs 44:14 122:22 145:10 149:20,20 149:23 153:9,12 154:13,17,22,22 154:25 155:1,22 156:21 157:3,9 158:17,22 253:20 253:23 254:17,23 258:25
long 25:12 64:4 154:25 188:19,20 200:9 201:21 204:1,8 209:13 216:20 219:9 220:16 224:15 247:25 251:12 255:4 264:13
long- 252:23
long-term 253:1,3
longer 15:24 113:11 190:12 191:5,12 191:19 193:7
look 9:19,22 11:22 16:13 17:14 18:10 21:11 22:9 24:4 25:9,17 26:22 27:4 27:5,14 28:25 29:6 29:15 33:1 42:25 44:13,14 48:19,25 49:23,25 50:2 52:5 52:6 54:23 67:10 67:16 82:19 84:19 89:19 92:13,13 93:14 94:3 108:19 113:17 116:20 117:22 122:22 124:6 138:21,24 139:19 140:8 163:22 166:2,18 166:20 169:2,6,14 169:19 173:9 176:12 186:15 187:14 199:8 200:3 202:7 204:4 206:14 207:14 229:17 240:3 248:24 260:11 266:11 267:3
looked 122:25 25 Ă

72:20 132:11 205:24 234:2 246:1
looking 3:7,11 4:9 20:20 25:2 31:11 36:13 38:4 44:25 45:18 53:10 57:23 58:15 60:6 75:23 75:25 76:4,7,16,19 76:21 78:4 83:1 85:12 110:1 118:5 140:21 165:19 169:11 172:15 174:11 180:15 197:4 230:5 233:15 234:3 242:10 247:13 249:8 264:20
looks 9:15 36:12 47:3 50:6 65:24 69:14 89:14 114:16 120:9 127:16 142:8 157:14 163:4,5 165:7 181:1 213:23 258:24 264:7
lose 92:9 197:13 260:7,8
losing 215:10
loss 34:8 103:13 197:2
losses 37:6,10 43:23
lost 39:7 69:14 261:16
lot 8:16 27:16 29:11 33:6 48:16,17 50:14 51:6 52:11 58:20 68:20 74:1 79:8 80:10 84:7 87:16,19 91:5 92:5 92:20 97:23 104:11,19 112:5 113:20 117:25 118:20 119:3,25 123:13,24 124:25 127:24 128:17 136:2 140:3,5 145:15 149:5 150:12,12 151:1 151:12,17 152:1 152:10,11,13 153:6,13 154:21 154:23 155:8 157:19 159:4,6 160:14 168:5 173:8,17 176:3 180:15 183:16 198:21 199:1,16 201:11 202:14 203:4,20 207:3 210:8,10 212:7 215:25 227:5 228:2 231:21 232:24 238:10 239:5,7,19 242:15 242:25 243:19 245:23 249:11 251:6 252:3,16,23 253:21,25 254:13 256:24 257:5,6,7,7 258:25 260:11 264:14 267:16,17
lots 238:14
love 53:16 82:21 116:7 129:11 168:9 206:21
low 43:4 51:17
low-risk 196:11 235:23
lowest 247:1 259:7
lows 147:21
lunch 21:15
luxury 175:12

First Version

95:19 128:20 130:11 145:25 147:10 159:21 162:3,16 172:13 182:14,18,19 189:22 190:14 191:2,7 200:15 227:14 252:5 254:25
news 27:22 38:20 61:17 153:21
nice 261:10 263:24 269:2
nicely 166:21
Nicholas 121:15
Nick 124:16 125:19 126:8 129:11 130:25 134:4 145:12 149:1 150:9 151:11 153:11 154:8 156:6 157:4 170:2 170:23
nine-digit 47:3
ninety- 158:20
NIS 47:23 49:24
NIST 48:15 160:18 173:16 231:18
nitty-gritty 207:7
no-brainer 226:13
noisier 159:10
nonbank 5:2
noncompliance 118:23
nongovernmental 256:12
nonprofit 86:21
Norin 172:11 174:14 178:13 184:24 192:2 194:4 207:3 209:25 217:14 219:15
norm 225:23
normal 159:11 225:13 252:22
normalize 151:9
normally 60:19
102:13 131:19 149:4 242:8
note 17:19 122:10 169:12 203:18 224:6
noted 177:5
notice 4:6 153:13 206:9
noticed 61:1 243:9
noticing 73:4 190:21
notification 153:23 236:1
notifications 184:10
noting 214:18
notion 127:20
NotPetya 262:13
novel 130:11
nowadays 239:10,14 239:17
NSA 155:24,25
nuanced 48:7 130:4
nuances 141:9 211:6
number 30:13 41:14 47:3,4 52:4 55:3 61:4 62:18 72:21 76:18 83:8 86:11 86:15 88:6 89:12 89:12,13 90:24,24 91:8,21,21 94:24 96:20 98:5 102:6 102:12 107:2,2 143:4 150:14 151:5 170:5,11 182:3,6 197:3 228:17 230:8 231:16,17,22 232:6,16 261:7
numbers 6:18 43:8 73:3 93:14 197:10 197:12 228:20,21 228:21,22 229:5 246:17
numerous 167:7
nurses 59:6 234:23
NYDFS 169:11

order 3:19 14:25
23:25 31:4 41:17
77:23 85:20 99:16
115:22 118:24
150:18 152:14
154:13 160:19
197:6 200:2
215:15 253:9
orders 201:25
organization 32:2
42:3 43:13 47:18
50:17 54:4 55:6
60:8,17 65:25 69:6
69:7 77:24 81:22
82:14 83:9,11
84:15 90:3 97:10
97:19,22 98:25
100:12 101:9
107:13 111:4,9
119:7,14,16
126:11 135:14,22
136:10 137:6,7
139:3 142:24
143:18 144:16,20
148:12 152:4
161:6,7 163:10
179:3,5 180:1
183:19 186:11,12
186:15 188:14
193:19 194:7
207:20 210:2,6,16
210:24,25 211:1
211:20 253:18,22
255:8 258:1
267:24
organization's
185:22 193:18
organization’s
30:24 89:17
226:25
organizational 99:9
100:6 101:11

First Version

probably

pull 134:7 182:24
pulled 82:13 102:14 103:11
pulling 82:11
purchasing 189:21
pure 185:7
purely 29:5 205:7
purpose 15:25 87:3 153:9
purposes 31:15,16 56:2 160:9 250:15
purview 56:9 108:24 180:14 217:20
push 53:23 137:9 168:10 234:15 267:3
pushback 39:9 106:12,14
pushed 41:3
pushes 41:7
pushing 40:7 49:18
put 9:18 47:5 55:11 66:8 73:23 87:10 90:21 101:17 156:20 183:11 189:8 190:25 200:17 210:10 228:4 238:21 242:16,20 252:19
puts 140:14
putting 44:7 46:16 156:12 164:10 188:17 200:24 247:11
Python 149:25

Q

QRadar 157:20
Quade 270:3,15,16
qualifications 11:8 11:15 46:8
qualified 10:14 11:1 11:2,10 13:1 74:14 74:23 75:3 77:1,5 77:17,21 78:1,22 79:12,22 80:16,23 95:25 101:25 105:17 119:9
qualifier 205:12 212:23
qualitative 55:14 196:16,25
qualitatively 55:8
quality 40:25 149:9 214:24
Qualys 140:11
quantifiabk **1645:8**

88:17 109:9,25
118:5 193:17
224:21 226:8
237:23

requirement

254:10,12
scanned 147:23
scanner 147:19
scanners 143:6
scanning 126:22 139:13,19,25 140:19 141:11,13 143:13 147:17

small/mid-sized 73:5 123:10
smaller 2:9 6:9 21:1 21:5,14 32:13,14 32:14 70:1 71:1,6 75:3 78:22 79:6 80:10,20 83:24 85:20,22 93:6,15 95:22 110:16 119:24 125:20,20 159:7 164:22 184:13 185:9 209:18 240:16 241:3 258:11
smallest 188:25
smart 134:12 146:24 187:22
smartphones 231:25 238:4
SMB 102:16
SMBs 115:5,10
SMBv1 262:24
SMS 231:7,10,13,14 231:19,25 232:5 232:12,17 234:25 235:3 238:7
Snort 149:10
SOC 45:17
social 6:17 47:4 61:25 91:11 228:20 229:4
society 31:3
soft 132:21
software 15:14 106:7 128:10,21 132:13 139:20,21 142:5 146:23 152:7 162:15 176:9 188:16 189:21,22 192:12 240:18 241:13 243:20,24 244:3 257:18 262:23
solely 184:15 215:3
solidified 130:19
solution 17:6,7,11 17:12 19:15 33:2 45:14 83:7 104:1
232:12 257:23 268:3,4
solutions 21:3,4 33:2 54:18 64:3,5 64:7 152:7 258:10 258:13 263:2 267:18
solve 167:18 262:17 262:18 268:7
solved 53:25
SomaLogic 157:20
somebody 38:24 64:10 79:5 119:15 130:3,7 133:1 135:21 140:12 143:8 144:15 147:25 151:12 155:5 157:10 158:8,10 165:25 166:2 178:2 186:19 187:9,11 187:15,16,20,21 195:18 208:17 212:2,5,12,20,22 212:25 213:1,20 247:18 255:9 258:15
someone's 113:14
somewhat 127:3
son 145:10
soon 148:17 235:8
sooner 244:21
sophisticated 246:21 256:12
Sorry 142:20 170:16 251:16
sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21
246:6 247:11 249:9,10 263:8
sorts 130:6 132:25 265:5,7
sought 8:17 85:16
sounds 49:6 68:22 146:13 250:13
source 30:13 39:5 140:13 157:25
south 243:19
SOX 158:3
space 53:7 81:10,11 81:22 94:21 107:1 125:17 147:4 150:12 178:17
speak 28:5 160:14 183:15 228:7 237:4
speaking 5:6 20:15 72:14 99:3 180:16 205:16 251:12 264:22
specialist 121:5
specialists 81:11
specialization 48:6
specialize 126:3
specific 11:7 16:22 48:17,24 66:24 68:6 72:23 74:18 82:15,15 100:15 101:10,16 105:5 110:25 116:1,5,16 128:6 130:1 147:14 185:11 203:6 208:16 215:22 223:21 246:22 257:14 260:10
specifically 114:25 131:11 142:23 151:3 163:14 183:19 193:5 209:10
specification 105:23
specificity 12:8 106:17 107:18 109:8 118:12
specifics 100:17,23
165:4
spectrum 7:11
speed 13:9 112:17 114:6 164:23 265:12
spend 149:7,21 208:21
spending 43:2,19 57:24 62:20 125:9 125:11 208:1
spent 92:21 173:11 257:5
spike 148:5
Spirion 228:16
split 211:13 214:19
splitting 149:25
Splunk 124:2 149:22 157:15,16 157:18
spoke 136:2 220:8
spoofed 245:8
spot 137:16 237:12
spread 261:15
spreading 134:5
spreadsheets 230:8
Springs 71:22 75:18
SSE/secure 162:22
SSL 107:22 162:21 225:3
staff 30:8 73:11 74:21,22 78:3 79:2 79:17 124:11 126:7 127:1 138:5 141:9 144:10 149:13,15,19 156:19 233:3 237:2,4
staffing 85:12 145:2 183:2 257:16
stakeholders 161:10 204:22
stand 211:12
standard 46:5 48:13 50:1,5,8 53:12 65:24 66:7 106:12 226:18 227:19,20 228:8 264:3
standards 46:7,11
47:13 49:23 50:9 52:12 66:14 80:2 89:9 161:12 229:21 237:19
standpoint 161:20 161:20 183:12 205:7 264:7 267:1
start 3:11,15 4:12 21:10 24:2,5 28:3 58:11,17 73:6 112:20 114:12 117:12 118:22,23 120:1,2 129:24 130:21 148:18 151:21 161:24 167:2 172:17,23 177:7,15,16 182:10 188:10 209:24 214:13 219:4 224:1,18 227:7 239:4 245:1 265:17 266:18
started 47:2 61:14 75:23 122:13 175:23 243:7
starting 4:13 39:13 39:14 46:3 84:11 114:11 115:8 198:11 245:2
starts 117:9 118:16 120:4,5 177:1
startups 176:2,4
state 54:13 96:21 153:22 172:12 182:18 209:11 223:11 241:8
state-mandated 233:9
state-specific 112:4
statement 114:2
states 112:4 113:17 133:19
statewide 174:5
static 98:10
status 14:11 96:4 99:23 163:25
stay 206:15 247:19 248:21 255:3

First Version

taken 59:18 70:5 120:14 171:3 191:5 207:9 221:3
takes 28:25 31:2 112:11 158:19,25 167:18 185:23 193:7 195:5 208:11
talent 80:15 82:14 129:14 151:9
talk 25:19 36:5 40:21 55:14 65:19 77:1 83:23 93:18 95:22 99:17 113:9 113:22 114:8 126:21 131:14 133:3 145:20 158:13 159:2 175:13 190:2 195:21 196:25 201:14 230:13 238:25 258:16
talked 27:19 64:21 65:7 72:3 74:1 92:5 118:1 123:6 151:11 167:3 220:5 232:7
talking 20:19 23:11 25:20 27:11 28:14 32:23 34:4,24 46:1 52:12 62:19 68:7 68:22 71:4 74:19 87:6 93:19 106:9 106:10,15 107:5 107:19 108:20 116:1,6 138:16,17 153:14 154:8 177:7 183:16 196:7 217:23 227:23 249:7 250:21,23 258:20
tampering 122:4
tap 83:4
target 12:4 184:1 259:5
targeted 143:5
task 75:4 100:11 236:23
tasked 106:2 193:24
tax 240:20
teach 32:18
teaches 222:22
team 36:18 44:11 49:3,4,5 74:18 75:2,9 79:21,22,25 80:10 81:20 109:20,25 110:15 110:24 126:1,2 137:5 146:23,23 178:2 186:8 187:6 190:24 191:2,8 197:15 202:23 204:15,18 210:18 210:19 211:14 223:9 237:2
teams 33:13 60:5 81:23,24 95:6 142:12 175:25 177:2 187:1,3 190:3,8 191:13,13 191:20 199:17 202:22 204:17
Tech 71:15 77:19,25 78:7 84:2,9,18 85:6 89:10 90:10 102:7,11 223:3,3 226:25 227:1,2,7 229:14 235:19 237:10,23 248:3
technical 68:25 72:8 106:19 183:17 196:20 201:18 233:17 263:19 264:3,5,7,10
technically 135:20
technique

60:15 90:12,25 93:18 95:12 99:20 102:24 107:22 108:21 109:5,7 110:13 112:13 114:12 115:5 120:4 127:18 129:17 137:15,19 139:20 140:16 144:12,17 146:1 149:14 152:3,19 159:13,21 160:25 161:3 163:21 165:15,25 166:2 169:20 176:24 190:12,21,22,24 192:20 195:6,15 203:23 208:6,15 212:6,22 213:2,3 213:18 216:19 218:14 225:22 227:10 228:6 229:1 230:11 234:21 239:25 242:23 244:21 245:18 246:25 250:19 254:2 258:4 264:8 266:3 266:16

theater 242:7,11,14

theirs 176:13

themes 177:6

theorem 247:14

theoretically 153:15

there's 6:21 14:2 16:21 19:5 24:6,7 25:5 36:8 39:24 40:5 50:14 51:18 51:20 60:4 62:12 62:12 75:7 92:7,12 92:20 94:24 95:5 100:25 101:2 102:17 106:12,12 106:22 107:10 113:18 115:14 118:15 143:15 144:3 151:19,22 157:17,19,20 165:10 168:7 173:8 189:25 192:5 197:12 210:22 214:3,5 215:2 225:1 238:14 247:14 258:23

thereto 96:11

they'd 249:3

they'll 23:9 24:11 31:21 41:5 106:5

they're 4:25 5:6,11 13:6,20 15:2,10,13 20:2 24:10,13 33:15 34:20 36:13 39:21 45:5 51:5 60:7 62:20 63:8,15 63:16 64:14 78:2 81:15,23 92:10 94:22 106:7 108:6 108:9 110:1 114:22 116:14,21 116:24 137:4 153:2,5 166:14 179:19 180:2 185:25 190:7,14 191:9 198:2 210:11 214:21,22 214:23 224:15 225:5 250:9,10 265:4

they've 110:13 152:13 202:1,25 211:5 215:11

thing 6:14 14:14 16:7,11 18:22 19:11 27:10 35:10 39:3 42:21 48:11 51:10 52:2 57:16 62:21,23 63:5,17 63:18 73:22,24 100:24 103:24 128:4 129:16 131:2,21 141:20 149:17 151:10,24 152:23 160:4 170:4 185:12 186:7 188:25 207:7 216:9 220:4 220:11 227:11 229:19 241:17,25 246:7 248:18 252:20 253:13 255:6 259:8 260:11 261:7,17 263:25 265:24 266:5

things 3:17 12:2 13:19 14:13 18:19 18:23 19:6,12 20:8 20:9 24:23,25 25:3 25:19 26:10 27:20 28:15 31:6,9,10 35:20 36:16 39:12 39:23 42:8 46:19 48:22,25 52:15 54:15 56:9 59:24 60:23 61:4,15,16 62:8 63:4 64:1,23 65:18,21 66:6,20 66:22,23 68:14,17 69:10 73:8 93:8 94:18 98:6 99:22 104:18 113:4,16 115:19 117:6 119:3,3 124:19 127:12 129:4 130:9,17,20 132:2 132:8,23 135:2,23 136:7 137:2 139:14 140:8,24 140:25 141:2,25 142:1,23 144:3,6,9 148:1 151:1 152:13 153:2 155:9 156:5,12 158:12 162:18,20 164:8,10,23 165:1 166:12,16,24 168:1,8,25 169:11 169:12 175:15 177:21,21 186:6 187:24 188:17 196:19 197:22 198:9 201:22 204:6 205:8,9,11 207:9 210:22 211:7 213:14,16 214:25 216:6,8 219:17 220:4 225:17 229:25 230:22,25 231:3 233:1 236:9 238:15 239:11 242:8 245:17 247:21 251:25 252:8 253:20,23 253:25 254:13 258:13 261:10 262:3 265:7 267:9

think 3:25 4:22,24 11:2,8,10 12:1,18 13:3 18:12 19:7 23:9 26:14 29:3,11 32:3,8 34:3,17 35:8,21 37:18 38:13 42:4,8,11,14 42:21 45:8,11,25 46:21 47:9 51:25 52:7,19 53:14,16 53:18 55:13,14 56:6,7 58:5,19 59:19 63:13 64:4,6 65:1 66:8 67:7,21 68:10,13 69:10 74:16 77:20 78:15 81:6 82:3,8,9 83:25 84:5 85:13 86:25 87:7,15,17 88:6,16,17,19 89:9 89:15 91:2 93:6 94:14,15,17 95:14 95:15 96:25 97:2 98:8 99:6,10,16 100:5,8,9 101:10 103:24 104:7,25 105:25 106:16,21 107:4,18 109:5 110:7,15 111:2 112:23 113:4,24 114:9,12 115:2,20 115:24 117:4,14 117:17,21 118:13 118:17,18,19 119:5 124:12 125:19 126:22 128:14 130:12,13 137:15,16 138:17 139:12,18 141:20 143:12 151:24 156:9 157:4,16 158:12 161:17 164:13,15,20 165:9 166:21,23 167:3,4 169:10 175:12 177:23,23 179:5 180:11 182:11,19,22 184:6,11,16,25 185:2,3,15 187:4 187:13 188:12,13 188:18 189:18,19 190:2,11,13 191:18 192:3,5 194:5,9,16,19,22 194:25,25 195:3,5 195:8,8,9,13,20 198:14,25 199:6 199:22 200:1,2,23 201:5,8,12,15,21 202:3,11,21 203:7 203:10,17,20 204:1 207:5,10,15 207:17,18 208:25 209:25 210:3,5,14 210:19,20,22 211:11,17,24 212:22 213:5,25 214:11,18 215:2 215:12,18 216:4 216:10,14,19 217:2,2,4 218:14 219:5,9 220:4 225:6,20 232:9 233:24 236:13 239:11,12,24 240:11 242:19,24 243:18 244:1,4,18 247:1 249:25 251:18,19 253:3 253:10 255:2,13 257:8 262:4 263:7

First Version

First Version

131:15 134:5 **1**36:15 138:25 143:11 144:22 145:23,24,25 146:10 151:14 152:13 153:1 159:10 162:18,20 164:2,5 166:7 167:10,14 227:14 227:15 229:3 230:5 237:14 248:14 250:12 252:7 255:4 265:20 266:10
we've 65:7 66:14 67:21 73:22 74:16 75:10 133:18 150:19 223:17 238:10 243:12 251:10 266:2 267:7
we'd 75:25 76:6,16 76:21
we'll 21:10,12,15,17 21:19 42:25 120:12 132:16 177:16
we're 3:11 4:13 11:4 20:15,19,20 21:25 21:25 25:1,2,7,14 25:15,16,23,24 26:5,7,8 27:11,14 27:15,15 28:7,17 28:22 29:10 30:6 32:7 34:16 35:4 36:21 37:2,14 38:14,15,16,21 39:13,19 42:5,17 42:19 43:9,19,22 44:16,22 52:12 55:1 56:23 58:2,8 60:4 62:19,21,22 62:22 81:13 82:20 83:1 85:2 87:6 90:12 93:19,25 95:12 97:20 99:15 99:18 100:1,2 103:11 106:15,17 106:21 107:11 108:4,20 109:2,3 110:21,22 115:5 116:1,5,17 117:23 118:19 138:6,11 144:19,20 145:20 155:9,9 163:22 164:21 165:12 169:15 170:25 173:4 175:12 179:24 183:15 192:23 193:22 197:21,21 198:11 199:13 218:20
we've 18:16 25:12 25:15,24,25 32:23 41:3,12 46:14 51:3 60:15 61:22 84:2 97:22 114:14 117:25 118:14 132:8 152:16 155:10 164:9 166:23 175:5 193:2 219:17,19 219:21 220:5 237:22 260:25 265:20 266:5
weak 116:12 133:5
weaker 139:17
weakness 254:15 255:14
weaknesses 127:19 129:3 130:15 142:3 162:11,12 162:14 168:18
wear 82:5
wearing 78:3 81:20 82:10
Weaver 121:16 124:19 125:22 131:1 145:4 149:5 153:12 155:14 159:24 160:4 170:3,21
web 95:8 136:6 151:4 226:15
web-based 226:12 226:16
web-type 136:22
website 102:15 130:8 225:6
week 131:19,19,21
weekend 148:1,3
weeks 67:13
weigh 217:4
weird 170:19
welcome 2:4 3:1,3 23:3 71:2 105:24 121:3 172:3 222:3 223:15
well-rounded 192:20
well-trained 62:5
Wendy 223:8,10,15 227:3 229:24 231:9 232:19 237:22 240:10 243:19 244:7 245:1 246:16 249:17 251:15,18 251:21 252:11,12 254:21 257:2 261:2,3 264:1 1- 76:; Ô Ǝ ž 2ű 7]Ǟ η Ô Ʈ