Bill Murphy ([00:03](https://www.rev.com/transcript-editor/Edit?token=X0nNj2ywf8urt5TGAhux_-3b3CheQxPhzgS02ExHEtCZYUvt07gW4lNm-VNA3jDlshK7fTKFffaiO19W3v8AaV2ogqA&loadFrom=DocumentDeeplink&ts=3.11)):

All right. All right. Roger, I want to welcome you to the show today.

Roger Grimes ([00:06](https://www.rev.com/transcript-editor/Edit?token=gAg7MgD8vpbqw2WHJPhiPfRFkwRNtO9FMGcUukFqKV7gM442cm0sHFRrfM0Zw2QUixdWnOlCinALkMfVT6HbiC0Jhuk&loadFrom=DocumentDeeplink&ts=6.4)):

Glad to be here. Thanks a lot, Bill.

Bill Murphy ([00:08](https://www.rev.com/transcript-editor/Edit?token=GEVshPKykuo7d9uXC4tcfqamMWpSwtTRV8YD9kuYSBZhR03ZE7xQn1GDMvQdSH7mDKptMjp8Zphax-WE5YqqwGbm69g&loadFrom=DocumentDeeplink&ts=8.12)):

Well, I'm very, very excited. You and I had a little bit of talk beforehand. And I think our listeners are in for a real special treat. I was bragging about you earlier today. I was talking to a CIO, and he's like, "Well, I really like talking about strategy. Can I talk strategy?" And I said, "Listen, we can go into the worms or we can stay at the cloud level metaphorically speaking." But I think our conversation is going to be wide and varied. But let me let you introduce yourself to my listeners.

Roger Grimes ([00:38](https://www.rev.com/transcript-editor/Edit?token=7l168NJQTweJ8UNNySK8DMo3SUSvHJg0zbB9N4FBauWRueR_sMit_5Boxs76cU36HwEf9RIrui_uNih3PmB-tMG_2rU&loadFrom=DocumentDeeplink&ts=38.1)):

Okay. So, I'm Roger Grimes. I'm the data-driven defense evangelist for KnowBe4. They're the leading security awareness training vendor helping people not to click on phishes. I've been doing computer security for 33 years, earned all these gray hairs. And I've been everything from starting out as a PC repair technician, network manager, all the way to BP of IT for a lot of years.

Roger Grimes ([01:01](https://www.rev.com/transcript-editor/Edit?token=xrDRlXKRlFSsy6jHlO72WFrFk7H5UY_p0Ei3xa5QrCd81GoWmeDRKCy-qpl1jXVsM1Gw1UcPGc1W0AYUO0UsqKaxbaY&loadFrom=DocumentDeeplink&ts=61.32)):

Always been interested in computer security. That really is what's captured my heart. I was even a CPA at one time, but I was a horrible CPA, and was glad I got into computers, but I've done a lot. And I've been writing a lot. I've written 12 books, over 1,000 magazine articles, a lot of it was the InfoWorld and CSO weekly security columnist for 15 years.

Roger Grimes ([01:24](https://www.rev.com/transcript-editor/Edit?token=MXvvBW-34Ky3ZJJxGfEEQ_y7EU0q_XFIiJ1R8oIFSF6q5GoPY1QY6YxBohxArv4T7pb2t41SWOcJi0ySh6Q06TIRP-Y&loadFrom=DocumentDeeplink&ts=84.13)):

And before that, it was even testing security equipment for them in the security testing center. And so, it's great that I've gotten paid to really look at, and review tons of stuff. I've done a lot as a penetration hacker, penetration tester for 20 years for Microsoft and bounced on my own companies. I broke into every company I was ever hired to break into in an hour or less, even though I had two weeks or two months, depending on the gig to do so.

Roger Grimes ([01:51](https://www.rev.com/transcript-editor/Edit?token=oyET0C2iRj__t8G4Lufc8ZTq21N_CDhdjkUa4L6y5X1QfeT54K8nbRSRw1Yx7uqC7KaefYvorNZakAU-6ACbiLEbSFY&loadFrom=DocumentDeeplink&ts=111.19)):

Except for one place, it took me three to five hours because the second time I was back there, and they closed most of the holes. But then I found out with a blank SQL SA password-

Bill Murphy ([02:01](https://www.rev.com/transcript-editor/Edit?token=ZkDfrGje01yhswAUvQAObxrcpYOleppzVCbfvKWQ-7cX5oL_xjQnLlBltEmEFJiVxypAyaM3BmADuesIB_vxIcfF0lc&loadFrom=DocumentDeeplink&ts=121.41)):

Yes. Now, I know why you and Kevin got along so well because he's... yeah, of course. He's one of the world's famous hackers. And that can be in your LinkedIn profile. I've hacked into every website that I've ever worked for to test in less than an hour.

Roger Grimes ([02:16](https://www.rev.com/transcript-editor/Edit?token=vLAf93B43ZFnTkIwFr3l2SropiRKkh2VO0It0opJaazNPUYSxKt6KlWqFe-JSZzfGZ6j7XqU9HpgYdzNiycHWmogekM&loadFrom=DocumentDeeplink&ts=136.36)):

What's interesting is from having worked with a lot of good hackers, and Kevin, let me say, I've been friends with Kevin for a long time, even wrote one of my first articles decades ago when he got arrested was people were like, "Free Kevin, free Kevin." I was like, "No, put his ass in jail." He broke the law. I have a very moral compass, and he broke the law, and you need to go to jail.

Roger Grimes ([02:36](https://www.rev.com/transcript-editor/Edit?token=VyJrAMWZhQh7WvbOP9JHceWAdeSgi1oBy43Ko00JQHjRepwEUNycqOHQBi6ogofL9zZGgPfQYagyAJ2hD5oStMax_wg&loadFrom=DocumentDeeplink&ts=156.53)):

And he didn't even steal money. He was just hack and hack. But when he got out of jail, he was in there for a couple years. He really turned, and he became a white hat hacker. And I was very dubious of him, but I actually wrote another column a couple years ago, and I'd met him, talked to him at conferences. And no, he's really made the turn. A lot of the white hat hackers like, "Oh, this guy is still hacking."

Roger Grimes ([02:55](https://www.rev.com/transcript-editor/Edit?token=Yg362S19LGcpETQvI5S2qFqdChD6ePuL-bjp5mJhrzsOGnFMnSb3K4ZkkvfD8faJld00fOor69FegsAaA9w8uVVj_DY&loadFrom=DocumentDeeplink&ts=175.8)):

He had made the turn. And I interviewed him for one of my books a couple years ago. And he said and I love it, he explains how it goes, "I get the same thrill from hacking as a penetration tester as I did as a hacker, but there's just more paperwork." And I was like, "Yeah, yeah."

Bill Murphy ([03:11](https://www.rev.com/transcript-editor/Edit?token=BDIiit49NqvNmKJ3dnB2IXGK-25ZyE5w9KRUHkvEnWo2Rocgt4U0Vsysncj-zhp4hbyO3MNEh-Qk6aus9X5pUSiZI4o&loadFrom=DocumentDeeplink&ts=191.71)):

That's perfect. I love that. One of the interesting things when KnowBe4 was just getting launched, oh, maybe not just launched, but it hadn't hit the cultural Zeitgeist moment that you guys are at right now. We went to a conference and he was handing out these cards that were made out of steel.

Roger Grimes ([03:29](https://www.rev.com/transcript-editor/Edit?token=q5RcCL1b3BqlM0CB2Ix1bvwEaW5Bn5KIsMOF-hM3yg2SSNL3vNgvcTmK-4SpL8NvKbbPwzyc3xjN_-tFsjFhCcCE52k&loadFrom=DocumentDeeplink&ts=209.42)):

He still does.

Bill Murphy ([03:30](https://www.rev.com/transcript-editor/Edit?token=XQVEr8mo_zc0uPgLCKqoPaSkfh_xp5qIeljn3q2cxs6vs-guJCLY29fpnEU29E5OmfTvZGD1ywzsvBEeFhYbdTBIwXg&loadFrom=DocumentDeeplink&ts=210.26)):

Oh, he still does?

Roger Grimes ([03:30](https://www.rev.com/transcript-editor/Edit?token=wmSNnSzmpI26UJpkGgy4ZdL_Syq_O4j1TtdkeMXw8nf6f2q7JsEc67enGqfwawlgA0GT9OcAQL5vdkpHNlKWIcSFvoE&loadFrom=DocumentDeeplink&ts=210.9)):

The lockpicks, the lockpickers.

Bill Murphy ([03:32](https://www.rev.com/transcript-editor/Edit?token=Vu_CQ1usdb6ENiYBfBLLnL6YO6mKqv69l3r9R2ewla38-gfB-abDtruakELNrouUYascvU_Koj9L83vgtW9vWEVAWik&loadFrom=DocumentDeeplink&ts=212.64)):

Yeah. Is it just him, or does the whole company have those-

Roger Grimes ([03:37](https://www.rev.com/transcript-editor/Edit?token=JVVvN-jae2vQTfHVHxuwlUADx4LU8XwgyL2TzDlJu87JShsFuGW-vqOycJd2-oOQo_5cUPsyEtW-SSAPxo4loTt7Wis&loadFrom=DocumentDeeplink&ts=217.93)):

It's just him. But I have so many people that asked me for them. I carry them with me. And I run out. But what's interesting is hanging around all the good hackers, let me say, Kevin is probably the best hacker I've been around. And I've been around a lot of good hackers. I always broke into everything I wanted to. But on a scale of one to 10, 10 being the best, I'm a five, maybe six.

Roger Grimes ([03:57](https://www.rev.com/transcript-editor/Edit?token=BE10fUZ0CuLxiVm5tWXF9Y7It0V5N64ecgd7ZZuQr_FESItUcqA3s5GTld6Ou1ta2ItLRegxKeSJvB1MdLUgM021pSA&loadFrom=DocumentDeeplink&ts=237.4)):

But let me say on computer security defense, I think I am the guy in the world. There is no one that can defend better than I can. I know it's a cocky thing to say, but it just is what it is. I know a lot about it. I know a lot about risk-based security. I've yet to meet somebody that knew more about... and let me say, the best, if you say how do I defend myself, I'm the guy you want to talk to.

Bill Murphy ([04:23](https://www.rev.com/transcript-editor/Edit?token=bPXOiMyqYrmAP2bQE3CeYQwFVqSR0Y6zbyZRDR29QC3rMY-IjGtQR-tv10x0Q5QSyzcPnxBqUGGDDGZlQFMFNig_xwg&loadFrom=DocumentDeeplink&ts=263.54)):

Yeah. I was going to ask you that because I didn't say that to everybody listening that I thought you were the world's foremost authority on multi-factor authentication. And you just wrote a book called Hacking Multifactor Authentication. And then, you just put a stake in the ground, and you said you're the best defensive security hacker, no, not hacker, but best security defender-

Roger Grimes ([04:48](https://www.rev.com/transcript-editor/Edit?token=9jh5te_XqfFeHr9FcxUTeHw-MBIum3XO-4elq4EKrNXSdKY-p0RrijD0o91P2d-JY5f26Xv69zUOpIUrFAT6_1FoWXI&loadFrom=DocumentDeeplink&ts=288.12)):

Defender.

Bill Murphy ([04:48](https://www.rev.com/transcript-editor/Edit?token=GqhTe2H51OiI_zB1Esms5NRRmOsiHG_O6y7l-RWmBD3JlbMhVllx0Lj2vF8R-kVhn4YWkBesN6_voY737kTLJ6dNcAs&loadFrom=DocumentDeeplink&ts=288.32)):

... defender in the world. So, we'll have to put that up against the best MFA. Well, I guess MFA now. I was just talking to someone about this that with people really strewn quite not just within the four walls of their business, or their remote offices. A CSO just told me recently that he had 35 offices, and he was securing 700 people.

Bill Murphy ([05:13](https://www.rev.com/transcript-editor/Edit?token=EUw53KOhg3ph_gz6N44RfWFCS_PFq0QAY-HyIMjpZs74bI1JvkSWHrSx_9zHcOdKkAVsWqD6Fd2mzWPT0qYO_U1oHe0&loadFrom=DocumentDeeplink&ts=313.01)):

Well, now, he's securing 700 remote offices. And this is a compliance-oriented organization. So, now, it's not just the digital, but it's also making sure that the policies around printing material, and using printers to print out documents. There was a whole set of things that they were used to within their four walls, that now they're going to do for people from home. So, quite interesting that way. How do you look at this new footprint, new expanded security footprint that we're in?

Roger Grimes ([05:45](https://www.rev.com/transcript-editor/Edit?token=yTKDkZE5O4vP3vRVy9eBnemrzxZZCvDkCwSQDBrMuqYCkvK7HCXIgKrANxIkVX1WQ1RnNqUkK4qpfd9814k6HPQwXGg&loadFrom=DocumentDeeplink&ts=345.98)):

So, the things that make people secure the best security stuff they can do, it doesn't really change whether you're at home, or whether you're at work. But I think certainly, everybody has changed, and very few people had... if you had remote workers, it was a handful of people or small percentage, usually for most companies to 100%. And people found out many of the things that worked wouldn't work well at scale remotely.

Roger Grimes ([06:11](https://www.rev.com/transcript-editor/Edit?token=i_GDvvxJrvJ78JRGnoBi2m3ph4yN-zKtWqEixe7gW0Ifp84LdFFW5IpSy9B882JhcEgT2bCBp40CwZSXEXkQW5mmdYM&loadFrom=DocumentDeeplink&ts=371.74)):

And so, you get all this new software, new VPNs, new this, new that. And I think that besides the challenges of just trying to secure those 700 offices, what a great quote, I think it's a scaling issue. But also, there's a lot of changes going on, and the hackers, and the phishers take advantage of that. I don't think if you sent to any employee that, "Hey, here's a new VPN software, because our old VPN software resistant."

Roger Grimes ([06:38](https://www.rev.com/transcript-editor/Edit?token=pQe3DWUPQl4yPETBulwvHT-MSR7uz2N4wOzmi00mahsj-J3ATVJrgEMOxWmrsyM5JeINB29a84XW9etWihZ71aH8870&loadFrom=DocumentDeeplink&ts=398.15)):

There is a lot of people that might fall for that type of scam, where if they're inside the office, no. When your job isn't really changing a whole lot, and all of a sudden, now you're in all kinds of turmoil. It's easier for things to sneak through, and somebody be tricked into clicking on something, and installing something they shouldn't.

Bill Murphy ([06:54](https://www.rev.com/transcript-editor/Edit?token=xqHmD1PnJpUfcaPS5ZjdN_UP6IE1MblQRc32CNBtY7QoGvYjRZC5-sFYbpp0YpDAGCzgiLLlvjPxaRzYCVMeY-ynLU4&loadFrom=DocumentDeeplink&ts=414.6)):

Yeah. Just because they're not within that four-wall environment with that same control-

Roger Grimes ([06:58](https://www.rev.com/transcript-editor/Edit?token=duu4folB_kbCHuTMwPOZQbfyt390F80GBtb8t2yYiLlbwMnV7f-s5iWf3r8jyyhXOVnrt90deejLmvK_5xNZ6qClG8A&loadFrom=DocumentDeeplink&ts=418.95)):

So, it's a double challenge, right?

Bill Murphy ([07:01](https://www.rev.com/transcript-editor/Edit?token=37NxYAbOs3Ix9V90Z3PZ1UkgMcdoch-NsirJ4h071oLcPK7kVdB8iT0rQVL_3N4p5wtqRNZek-N087ryRC3ihXDlyGM&loadFrom=DocumentDeeplink&ts=421.49)):

Yeah, for sure. And you and I talked a little bit about risk. And you even just mentioned in a minute or two ago. I'd love to get your thoughts on this because I think we're security professionals now. We've been currently in this market that has risen for the past decade, which is unprecedented. And then, all of a sudden, now we've got the bubbles been burst a bit with the Corona. I'm thinking that risk is now going to be first and foremost. And I'm wondering what you think about that?

Roger Grimes ([07:36](https://www.rev.com/transcript-editor/Edit?token=E-J5FktbPqsYkGR71Cr9ZoS7ScDxSYyhkPjQzJ_XD1gUNxDDa3tlpGTROcTfcTpg4wjDJ5cRh6bwxa7BvjrRYVRLhGI&loadFrom=DocumentDeeplink&ts=456.62)):

Well, here's a wild thing. Let me say, not to always push my books, but I consider out of the 12 books I have, there's one called data-driven defense, data-driven computer defense, came out a couple years ago. That's my magnum opus. The other books don't matter near as much as that one. And if someone says, "Well, Roger, which of your books should I read?"

Roger Grimes ([07:53](https://www.rev.com/transcript-editor/Edit?token=b4cwPfoEmREWg-VwycSSWcnoYADvYTCv7ZiXf6NUT9AO9xriyaehjwJBmQIdTHkxzm7ZdHySA0-boEn70fnuHkfwoxo&loadFrom=DocumentDeeplink&ts=473.06)):

That one because the lessons that it teaches in there about how to do better risk-based security underlies everything else. And the vast majority of companies do not do the risk right. They're absolutely horrible at it. So, social engineering is responsible for 70% to 90% of all malicious data breaches today, unpatched software, about 20 to 40%. And then, they overlap each other.

Roger Grimes ([08:17](https://www.rev.com/transcript-editor/Edit?token=vOKURmugYfEvclKvylqNAkM6h7DK_kK0FLxZWrNSNxB8qYWcfbVCxy8NSJsmbnEWF4F94o_5s2iDolpIcab8yn2gL8A&loadFrom=DocumentDeeplink&ts=497.28)):

Everything else you can think of, password hacking, insider threat, whatever, it only accounts for about 1% to 10% of the risk in most organizations. If you can think of how somebody has been compromised, if you've even read in the paper on your own devices and computers at home, it was probably social engineering or unpatched software.

Roger Grimes ([08:35](https://www.rev.com/transcript-editor/Edit?token=xO7ycH51L6I3uhnUqeKCnodqHhFqpdrn8rEC_bnfxj_BPIXkZEUAUwMwLP8y5gUBH8_uc2Y7Cgd4rS1yb3C2dDVLajk&loadFrom=DocumentDeeplink&ts=515.6)):

And yet, the average company doesn't devote 5% of their resources to fixing those things. And they actually aren't fixed. They're never fixed. They have been the number one, number two, they change position sometimes, but they've been the number one, number two ways to break into somebody's network or device for all 30 years I've been in computers.

Roger Grimes ([08:54](https://www.rev.com/transcript-editor/Edit?token=SWNK_qfyk8ibJy9cAoy5YCIiU7zxJwBmF-pwD7B84fSAZQNVBKSbIgLmfgNRz-GBnXB6Yu7ctcAUV4F7NT9HRKe6L7s&loadFrom=DocumentDeeplink&ts=534.08)):

It's not a surprise, yet you have all these people, "Oh, I got to get the latest endpoint detection. I need to get the best intrusion detection. I need to get this thing and that thing." But they're not concentrating on just doing like, it's not a surprise. I feel like I'm Warren Buffett telling people to buy low and sell high. And then, you just can't get people to do that.

Roger Grimes ([09:12](https://www.rev.com/transcript-editor/Edit?token=hv9HAPldwbvd2eAErayDNut8NC8o9ZWFVJAKwevWNBKud7trHpH6bm3iidnMLtchPueGKZrfsMDNelgY2BEkvSU5jvI&loadFrom=DocumentDeeplink&ts=552.67)):

I'm literally saying you should patch your software, and not get tricked into doing something bad. And that's it, and people don't do it. And they're like, "Huh, we got hacked again. How was it? Oh, social engineering unpatched software." And then, they go out, and they buy $100,000 appliance device that does some fancy future detection thing that they've been sold.

Roger Grimes ([09:33](https://www.rev.com/transcript-editor/Edit?token=VABjM6J6VH0y9pnEShzYQMu2ocLh3zQOQAQR1wYW78rL1ad1O9grOdkkUqd2sjErOD_2-KkxC472tw2W_toRA_3HPrg&loadFrom=DocumentDeeplink&ts=573.67)):

But they're not making patching better, and they're not working harder to stop. They're like, "We're trying to stop social engineering." I'm like, "Well, are you really effectively aggressively because it's your number one threat?" No company I've ever met has treated it like the number one threat or like, "Well, we're worried about ransomware."

Roger Grimes ([09:47](https://www.rev.com/transcript-editor/Edit?token=JtzKFn86VsorpN5Tm7bfXvRsS7tpHRjwtacybDuabTCvaa0tbSuD81rv6ujs9kf-32cAGABAxodJ8vzyAETrGHc8vXM&loadFrom=DocumentDeeplink&ts=587.73)):

Ransomware is an outcome of you not being patched, or being socially engineered. Ransomware is not your problem. That is an outcome of a problem. And people don't focus enough on the route exploit entry points, there's 10 of them. And there's only 10 ways of hackers and malware break into your environment.

Roger Grimes ([10:08](https://www.rev.com/transcript-editor/Edit?token=cc1aYztPuSJNBvakwdYjUFDIWuXBMBK9VVvmJPQBK7xhyAXy7tHdiB47JpOjL1Z4P8C9imGmSWtf-f51ngOD1fUCxWk&loadFrom=DocumentDeeplink&ts=608.91)):

And it's like every computer company is like, "My house is broken into again. My house is broken into again. My house is broken into again." And you're like, "Well, how are they broken in?" They're like, "I don't know. The thief got in the bedroom. The thief got in the bedroom. The thief got in the bedroom." But if you don't know, is it through the door, or the window, or maybe they learned.

Roger Grimes ([10:26](https://www.rev.com/transcript-editor/Edit?token=QhEq3jW8q5b3FiMnQ3mb6CvoNqbL601UHKTXzD2yAVSP3b1k3K8k0ybT0XTVpcSrctcYzxccGFCWUCJ5x7aU9u0bXi4&loadFrom=DocumentDeeplink&ts=626.13)):

Let me tell you how bad it is. They learned that the thief is coming through the window. Every time they've broken in and it's been through a window, I'm going to go out and buy a door with more locks. That literally is how bad the... we have this entire industry that seems like it's matured with the most immature risk model I've ever seen in my life.

Roger Grimes ([10:47](https://www.rev.com/transcript-editor/Edit?token=UgRIh6k9M8-pd4sUZr3euXtL9_uuD7weeVnBSNkrbBC07W3V6-7r-r5pDjdtiFhT7Uqk30tFzGtwE3peiq8qcKgsKME&loadFrom=DocumentDeeplink&ts=647.06)):

We were told computer security is about risk management. But there's almost no consideration of risk in most of the decisions at all. Someone reads from a book and goes, "Oh, this threat." Let's say Meltdown and Spectre. Meltdown and Spectre has the most highest risk exploits, impacts all CPU chips made since the 1990s. And if you don't patch it, you're at high risk.

Roger Grimes ([11:07](https://www.rev.com/transcript-editor/Edit?token=fPS06UmEgY1jHrtslj6mo6nHINKNT5z2GHUNLv17MxdUO2IoGi1bbSyVaIlRmo0iNkij06d_TgJKrQ2i5u-PB_yAaiI&loadFrom=DocumentDeeplink&ts=667.43)):

And if you're on a software vulnerability report, software patch vulnerability reports and say, "Meltdown and Spectre, critical risk, patch them now." There has never been, as far as I know, a successful public use Meltdown or Spectre exploit against any company in the entire global world.

Bill Murphy ([11:24](https://www.rev.com/transcript-editor/Edit?token=xSZ1o2dY3y_1kcUKNU7UcKcQ_gTK9l1ZUGeJd7okSVe3CTLH_URD16FXG8cjYiVeqgZZ-gCOrUXAMc4eJnbTWDrUxAw&loadFrom=DocumentDeeplink&ts=684.69)):

Yeah. It's interesting. I don't think people have a problem with the Microsoft patches. But I think a lot of problems with the third-party apps. I think the third-party applications, especially the ones that introduce system instability, so it almost becomes an availability problem as much as a patching problem. What are your thoughts on that?

Roger Grimes ([11:44](https://www.rev.com/transcript-editor/Edit?token=pvZF2_Jyrw6TMYxzRLE44ncG0kkr3hot2_LJ5-T6VoJ42DxUkc9zc-dTGzNZrz3Jib59suxgPIOSSw-BSeKwfO6tCQs&loadFrom=DocumentDeeplink&ts=704.09)):

Well, certainly, but let me say this, again, if you look at the data, only 2% of exploits that are out. So, last year, we had 12,174 things you're supposed to patch. The year before that, it was almost 15,000, the year before that, there's almost 17,000. So, 12,000, great, we should celebrate. Less than 2% of those were ever actually used ever in the field. But most people don't know that.

Roger Grimes ([12:05](https://www.rev.com/transcript-editor/Edit?token=RbY0YkcFQ9NgOWDgopRUDLUkuXVBF1n23Fr8LDw9koTkC0YbTfMWnpMPakn6mR3g2BqnN2hSvHC51wIpFXDpMs9Ihps&loadFrom=DocumentDeeplink&ts=725.84)):

And so, they're trying to patch it all. And so, if you have a patch management program, they got 5,000 things they want to patch. When the reality is, if you focus better at 100% patching of the 10 most likely things to be patched, you'd be far better off.

Bill Murphy ([12:17](https://www.rev.com/transcript-editor/Edit?token=9gjm4creYDpl5NyflqQcyQEvJMPvGgNhOnUpvXG2tiIspY97YxKhUZoLdfjHsPET1LCfoqlBgv_ETaFl1_hWhkqcQLc&loadFrom=DocumentDeeplink&ts=737.76)):

So, the 10 most likely things to patch are different than when you mentioned earlier, the 10 ways that I could hack you?

Roger Grimes ([12:23](https://www.rev.com/transcript-editor/Edit?token=sr5tFtI8NhmrjwfrRjLXYoaowi4Uiw6jdulUna3jq0NDY1XQTfwPEsiaRqle052Yv9neMUfwn8AEd4R1NOCAQlrF2yk&loadFrom=DocumentDeeplink&ts=743.56)):

Yeah, yeah.

Bill Murphy ([12:24](https://www.rev.com/transcript-editor/Edit?token=Ty0JzM8ldhTuULsZyk7qFAzyq6r2zhOaXKBc1QSLwKzbYxUlV4eX67w8KVGhfwYCgWiVogcOoxR0SVQ4XJRl7OqwziY&loadFrom=DocumentDeeplink&ts=744.41)):

Okay. So, it's really interesting, you're almost saying that you need to take an 80/20 analysis, use a Pareto principle, and look, where would you go to find that? If I had to do patching, I'm a new CIO, or I'm an old CIO, for that matter. I'm at an organization with 400 systems strewn across Azure, AWS, on-prem, collocation facilities, and I've got to execute on patching. Where would I find my top 20% if you were running the show?

Roger Grimes ([12:57](https://www.rev.com/transcript-editor/Edit?token=52W835IriloObsY9KEB9G13BhghKgwet52fD5KJR9uvfSbolx2q9KBzv_UmBLgEk-W2edcNaQFcRkGflp0N-Vw_bBl4&loadFrom=DocumentDeeplink&ts=777.67)):

Actually, when I came up with this idea, that data-driven defense, it was 20 years ago, and I wrote 10 or 15 columns, and I wrote a white paper for Microsoft, and then I wrote this book, there was nothing. And [inaudible 00:13:07] webinars, and talks, and book covered the best. But there's actually entire companies now, just off the top my head, Kenna Security that I like, and there's another called Risk Based Security.

Roger Grimes ([13:18](https://www.rev.com/transcript-editor/Edit?token=yhcBRuSPw8BraP87zPibIRP6Hh2o_9PLj2jKcxAjCN2v4e6-xVneZHXmaaGx3KkAVtKjuu-dUoWOnM4JpFKbOlCQg0I&loadFrom=DocumentDeeplink&ts=798.18)):

That companies, if you interact with them, they'll actually measure and determine what is the real risk. You don't have to worry about your cafeteria program being compromised. But if you're still not patching Oracle, Java, that's a problem. And that's the issues. If someone talks to me in 10 minutes, I can tell them how to figure out how they're being compromised, and how to close those holes.

Roger Grimes ([13:43](https://www.rev.com/transcript-editor/Edit?token=ZTyV4gV7mK3nfdLZnFn4-kZN68Y-m7V4UP5shGFmCErpvbam0EkxbLm-seirHulzK9wvMPY8oqGu4oods4sv1UQ2Vzc&loadFrom=DocumentDeeplink&ts=823.93)):

One of the biggest numbers that no one ever gets is how long did the malware dwell before it was detected and removed. Because it's not to the antivirus' interest to tell you that, "Hey, it took us three weeks." The average ransomware program is in up to eight months before it's detected, and removed, or goes off. So, when an antivirus detects something and removes it, your risk is gone.

Roger Grimes ([14:04](https://www.rev.com/transcript-editor/Edit?token=Ttw77tHkO5ZHYVDel88j30SKHViyh2BR1p7w3c4dfg8PRgr4IBpCX79aeRFelwn2BGW009koAeJF9VMZjsnkvSw7jhs&loadFrom=DocumentDeeplink&ts=844.3)):

Most of the risk is when it's in your system, collecting passwords, and getting ready to encrypt things. But software doesn't tell you that. It doesn't tell you, it's just like, "Oh, we got rid of this malware program." So, I tell people, a little hint I tell them is enable application control software like AppLocker in audit only mode so that it detects every time there's a new execution.

Roger Grimes ([14:24](https://www.rev.com/transcript-editor/Edit?token=Z7q5lcXvzPuh7O2AJDFga2J9NCr5F50rkJv3rxGhfBisQZZ2aLtk23sdGI4ckZW1Hi0OA4pjn3SguQlwlyTbPVr13Bw&loadFrom=DocumentDeeplink&ts=864.71)):

And then, every time you have a malware detection, compare it on that device or workstation to when that execution first occurred. So, the malware detects it, removes it, and it's always got a name. And you just search back in the AppLocker log, find the first execution, and you know how long it was living on that computer. And was it one second, one minute, one hour, one day, three weeks, eight months? And you can start to literally, in a day, I could help you set up a system in a day.

Bill Murphy ([15:09](https://www.rev.com/transcript-editor/Edit?token=pSVekcNDBw1AViSeGkh9AQC2w8Yfx4LCyJujDq_B4AXeaGiyBwo538CSukVr84_ksTASeCUCr2BzFj873-QgER9uWgs&loadFrom=DocumentDeeplink&ts=909.01)):

So, is AppLocker a... I think if it as a whitelisting system, you can whitelist. But you're saying turn on audit only mode first before you turn on. So, it's really-

Roger Grimes ([15:28](https://www.rev.com/transcript-editor/Edit?token=DJI14O0KmsXZG51vZPDy_a_BtAMd2kKwgL2mkhwvRfcVm4_75tNSlyGPF8-Qt2eDHEfow8pa5U7kT33rqT9mJoH7iJo&loadFrom=DocumentDeeplink&ts=928.94)):

Yeah. Most people when thinking of application control, which is whitelisting and blacklisting, they think about the enforcement mode, the blocking mode. And you really have to be thoughtful about that, and you're going to make a lot of people mad if you don't do it well. Audit only mode, when I turn on AppLocker, in particular, in Microsoft, no one even knows it occurs.

Roger Grimes ([15:47](https://www.rev.com/transcript-editor/Edit?token=lhVp2n7flLvwy-ww_yekFSoLAgEAHZHAyGEK-loG9H3INUkf2NiOztHY_kyEq_KplqGoY0E_ro5nedI-TgmsikSxMIs&loadFrom=DocumentDeeplink&ts=947.53)):

We turned it on across Microsoft, and nobody even knew, not even the computer security people, because it's an invasive. But it's recording the events. So, you can actually snapshot a computer and say, "This is all the legitimate stuff." And then, AppLocker will put a different code out for anything that's installed or executed after that snapshot. It's event error message 8003.

Roger Grimes ([16:08](https://www.rev.com/transcript-editor/Edit?token=xuGI5M_-Qx85nqdOrqlgKBpJ2CsdW3veli7ROTBdzSJ2ePWCvVmOGwEYUlu3xG640hH43zuMv94ji7lKnnVWp6dNtpc&loadFrom=DocumentDeeplink&ts=968.23)):

And you can literally, every time you get 8003, you can pick up that event, go in the database. Every time you get a malware detection, go look in that database, even fireless malware. People are like "Oh, can you detect fireless malware? Yes, yes, it works." And then, you can determine what's my dwell time, because that's really your risk. And you can track it per workstation.

Roger Grimes ([16:26](https://www.rev.com/transcript-editor/Edit?token=4GejXUS5Xr0HGjrdXTTbZ-A3v_5qUsfe_1E1MDDngVPSwbi_z0T2sZ-03Sl8_9OQ2p8MiyU4EHIWh6Kb6w5OT2bpHqU&loadFrom=DocumentDeeplink&ts=986.97)):

If Bill's computer gets compromised, if it's detected and removed in a second or a minute, not as much stuff I need to worry about. If it's on Bill's computer for three weeks, Bill has got to start deciding, "Okay, it could have been capturing my passwords, keylogging me, where have I been, what did I do?" And if it's on the CEO's computer, how long it was there?

Roger Grimes ([16:45](https://www.rev.com/transcript-editor/Edit?token=L3QRcuHVHzQXut3DeABaaOA3dcEbs_4RIS8O18l5P65D0uN-Pxf_R9RX4QahDvjQxM-5o5AYY5reTUxstz4qkgRJ9IE&loadFrom=DocumentDeeplink&ts=1005.68)):

And you can collect aggregate statistics as well and go, "Okay, we're using the software program, this AV or endpoint detection, and our dwell time is starting to increase." Well, if you have the data, you can go to that vendor and go, "Hey, our dwell time for this ransomware used to be really good. But now, it's starting to lengthen." When you give them the data, they'll actually respond and fix that problem.

Roger Grimes ([17:07](https://www.rev.com/transcript-editor/Edit?token=6-SoOHI10kZasddTBuwqTmPyRiu45iADZTEsc1Xd2u5E6MxcmevyXNPXfBmAzYO5K1zXDkgXKE34wnaiAIcumEs8QUY&loadFrom=DocumentDeeplink&ts=1027.24)):

And it's amazing, it's free. All it takes is picking up events from two different things, putting them in a database, and running the script that does a comparison.

Bill Murphy ([17:16](https://www.rev.com/transcript-editor/Edit?token=IQ6fF7qVIV9CXnpNbmCVBznwh6bSgg8R4uOIoYkqsNAhJ6W7zDOB5kQk_GSQWzxAkt7Pd08iKdaUA9bJ9PgxRrp0-_0&loadFrom=DocumentDeeplink&ts=1036.15)):

Pretty easy, pretty straightforward. And so, that's how you're dealing with zero day versus a signature-based. So, basically, what you just described was with the file list and with non-signatures, how that particular product is just doing a compare between system states.

Roger Grimes ([17:36](https://www.rev.com/transcript-editor/Edit?token=TRSLWO9rucEJpm6PcX1RrWfXeyROTmvdV2P5c-6sDp5p7Kh-MvfwiqQII0cpgPixuutsNIvS61qT2waNSrvc_rJ3Fnw&loadFrom=DocumentDeeplink&ts=1056.88)):

Yeah. And now, it's not always going to be zero days. It could be they downloaded BearShare, or something like that. But you could investigate that at the very least. Actually, Bit9 Parity is the first one, I love what they did. They're now owned by black guys, or something like that today. But the Bit9 Parity product is first on my file list.

Roger Grimes ([17:57](https://www.rev.com/transcript-editor/Edit?token=83JXq1ePTjHp2uH1TloXCp0DIDTK9JA_9lWderoikulRTO4vEFtVDX2aXgkOMojcyqPKuV82mNJ4NZ1k6m2S3n9qXSQ&loadFrom=DocumentDeeplink&ts=1077.07)):

It actually ranked every, like if someone executed BearShare, and BearShare at that point in time was being used by a lot of malware programs, it would give it a higher risk score. But what I'm saying is the AppLocker for Windows machines, it's free. And literally, you can set up a system in a day. And my thing is you got to be careful, because if you're following every new execution, there's a lot of false positives in there.

Roger Grimes ([18:24](https://www.rev.com/transcript-editor/Edit?token=VoEIzJg10N4cghvfLoVTEF6t0mcioYFDmufuaspRTYbNsRfWj0AvFBVOCP0xYyQP5Jwn78VdVm-5xLqS_2vOpMhMpXM&loadFrom=DocumentDeeplink&ts=1104.2)):

What I'm saying is, if the malware detector finally detects it, at least you can determine dwell time, but you could do what you say, Bill. But that takes a little bit more intelligence. That may be too much noise trying to figure out if every new execution is malware. But certainly, if you followed that up, and looked into it, you could detect zero days and new programs.

Roger Grimes ([18:45](https://www.rev.com/transcript-editor/Edit?token=q54B_7t0dW1wzAuv51XYzYNLgbxlPYy57RSPjNm_w6tCEtB4PntNDlqZquYeJMgf1h-rQ0bAZ8yiNXK0Oe1MN7NERxM&loadFrom=DocumentDeeplink&ts=1125.71)):

But at the very least, getting dwell time because that's your risk. But almost, if I go to somebody go, "What's the average length malware is in your company?" The average answer I get is they're like, "Oh, we don't have any malware in our company, or it detects and removes it." I'm like, "Have you ever been to Google's VirusTotal? They get 72 antivirus engines, and they never all detect anything ever."

Roger Grimes ([19:06](https://www.rev.com/transcript-editor/Edit?token=hbTlIr8dDhSRqUgJtje8g9fIDAWReqq7vGD-BTYPzxXPq5uLjPMCw2Zerj3yZY8y-5ctDBBlkw-RQaZUG4drnLGt5PU&loadFrom=DocumentDeeplink&ts=1146.44)):

If you get a 30% hit rate across all the antivirus engines, you found a program that's well known. Every bit of malware that I work, almost everything is not detected by anything for weeks to months. And even after a week or two, it's only detected by a couple of things. So, again, dwell time is a big deal. There's a lot more malware hanging out on people's systems than anybody knows about. And why? Because they're not asking the right question, and they're not putting instrumentation into their environment to detect it in the first place.

Bill Murphy ([19:35](https://www.rev.com/transcript-editor/Edit?token=Iy-wooP7fT4ja4Hl0id6rQeZVmyERuwdPW5OMyGET4cbm0oZypAO4n9sZH1-SL3F69JjVIgVjX3pTzHZ_2QYRXt-iQg&loadFrom=DocumentDeeplink&ts=1175.67)):

Yeah. You have to assume, I think one of the greatest questions is not to keep it out, but assuming that you have. Asking the right question will put the right defense in place. So, if you make the assumption that I am hacked, that I do have malware, then you would buy a product, that would mean you'd have the right instrumentation on there.

Roger Grimes ([19:56](https://www.rev.com/transcript-editor/Edit?token=gqwnLnJG3gNcMwK74pLgqlZcHF9ZFx3pux4nuecIQvaFBOIx7wjirzc2zWLrbHemIEVGvJ1-1lDGPWoAUF89sAc-dXQ&loadFrom=DocumentDeeplink&ts=1196.07)):

Yeah. Albert Einstein said if you gave me an hour to answer a question that my life depended upon, I would spend the first 55 minutes trying to think about the right questions to ask. For if I asked the right questions, I'd be able to give you the answer no problem, something like that, paraphrasing.

Bill Murphy ([20:10](https://www.rev.com/transcript-editor/Edit?token=c1IRDyGcqX6rMT3aODcG7DrDLKuvCINs4pMUdnOgci6hMaaGP5PHgxI5TERZ5jJCNqQf3bPLnpMXiwuKM2LeXYNdcjk&loadFrom=DocumentDeeplink&ts=1210.84)):

But nobody wants to ask that question because especially in front of their boss, because their boss hired them to be even, the best defender out there. But if the best defender comes in and goes, "Well, we need to assume we're breached, then it becomes system availability, how quickly can we recover? How can we root out and find? How can we-"

Roger Grimes ([20:29](https://www.rev.com/transcript-editor/Edit?token=tuqax5eJd_mSax5Y__oyuuGz_GT18YgSUsRms85RLHJ2C4PnBSl8JKUFn8JdQ0tePnp0NBhAgmqMoxUaFqA791YphBA&loadFrom=DocumentDeeplink&ts=1229.43)):

Are you ready for this? I hate to assume breach. Assume breaches for losers. We do have to assume breach. Assume breach is you're either compromised, you have to assume you're either currently compromised, or could easily be compromised. And we do have to do that. That is the right mentality today. Because we're not correctly, or more strongly stopping stuff.

Roger Grimes ([20:51](https://www.rev.com/transcript-editor/Edit?token=ijtgxkSpmqt-mg-AEsRC9xErt-m0nHBeDy9Oo8RezDaE7use2NAID_H7JQjLalb2w08VCwKSC2Ib1Gbl_JGMR2U8u5k&loadFrom=DocumentDeeplink&ts=1251.29)):

You can't put 5% of your resources against 70% of your problem. And think that you're doing a good job, and wondering well, how come we're still being compromised? We got hacked again. I used to be amazed. I would go to customers, and I would say, "You need to do this. You need to patch Java. You need to change this, configure it, whatever it was."

Roger Grimes ([21:11](https://www.rev.com/transcript-editor/Edit?token=9u07SkNu6AT6XmWnfJ4C3P7GgdbQc-3v_6N69nZGwT5Ok0wGx-935uc5cFKVIEVXh563TJ_8Bl58k-sw6L8ZOKzBhco&loadFrom=DocumentDeeplink&ts=1271.49)):

And I'd say every time you pay me, when I was with Microsoft, there's this $40,000 engagement. And I had to give you an 80-page report with 50 things that were broken. But I went out of my way to go, "This is the thing you need to fix first." Never but once in 12 years with Microsoft did the customer ever fixed the thing that I told them that was number one.

Roger Grimes ([21:32](https://www.rev.com/transcript-editor/Edit?token=NIpzQKQhnk79g0sJyJEZr0IkNOTTb3QkGY9vigfb7FizA-6MkFyTOScAKGV7_9Yccm3iGKfQbyVKRDAIBL9iMcf0ohM&loadFrom=DocumentDeeplink&ts=1292.56)):

And they would be compromised, there would be 100-million-dollar fines, CSOs would be fired, CEOs would be fired. And the people that came in to replace them wouldn't fix it. They go, "We can't." I'd say you need to patch Java. That was the big one while I was there. You need to patch Java. Java in 2005 was responsible for 91% of all exploits by itself.

Roger Grimes ([21:51](https://www.rev.com/transcript-editor/Edit?token=RLMXIyTfnKJJuWOziM8KzKhkuJRRkZx9Xj2FgtmyR9J1smn1cyId9MLVtIDiApnstR2AXxJTXJwfLDmyE2xFkmrUM3M&loadFrom=DocumentDeeplink&ts=1311.27)):

Meaning, that if you patch just Java, almost all your risk is gone. But they wouldn't do it. I'd come back in six months or a year, and they wouldn't do it. And I go, "How come you like, what breaks things?" I'm like, "Well, your answer shouldn't be binary. It shouldn't be, huh, we can't fix it, it breaks things." There's a lot of things you can do besides just give up. And then, like, "Oh, we got broken into, probably Java."

Bill Murphy ([22:11](https://www.rev.com/transcript-editor/Edit?token=-4bZeKfySF29GOa9Eip2JhoFGkNUd1RpvkIszId92fx5zfX1THO1h8jEVO_GjbydNAaX0gBbUGCbHbI1nrI0YO_SpIs&loadFrom=DocumentDeeplink&ts=1331.68)):

So, I feel like I'm sitting in front of an Oracle as some respects. And so, you just wrote this book, and I know you have this other magnum opus, the data-driven security. But I'd like if we can ask you a couple questions about MFA, multi-factor authentication. And you have a general thesis, let me just start there is that, obviously, your general thesis is in the introduction of the book.

Bill Murphy ([22:41](https://www.rev.com/transcript-editor/Edit?token=L2iC0ksDo_3-nJcy0Au1QMV_dmHnPMTvQnYftZGKFtR6xAcLk-bVzbjLx-zNb-83I7Yspdi3TvJWJ3FLkJyyXZPeTfM&loadFrom=DocumentDeeplink&ts=1361.58)):

But then, we can get into some of the mechanics. And people can go buy it, and getting more the specifics. But I really would like to know your general thesis on this because I do believe MFA were being sold a bill of goods. And I love to get your general thesis on multi-factor, and then we'll jump into some of the details.

Roger Grimes ([23:00](https://www.rev.com/transcript-editor/Edit?token=KF5lv8oG19SzILTwbViwNKOdh1pWiz56kEC2BqNiRd8CSlWrfWjp28LQZl7qiLMjgMaoE7oZsiLyTJ9Adny8muUsk9g&loadFrom=DocumentDeeplink&ts=1380.73)):

Okay. Also, it came about because actually, Kevin Mitnick, he did a demo a year or two ago about him hacking MFA around LinkedIn.

Bill Murphy ([23:08](https://www.rev.com/transcript-editor/Edit?token=fBAhZuivOwwff82sthwDYPerlWBRKW_sAmI8iYrs8awWdVmbWpgnJBPgHPlOb9vlN-IWZjn6D-PO3khj8HdOBWnC7PE&loadFrom=DocumentDeeplink&ts=1388.97)):

And I know that you have the link for that in your book. And so, I'll provide that because I saw it on the Kindle version. I'll provide that for the listeners to go look at that.

Roger Grimes ([23:18](https://www.rev.com/transcript-editor/Edit?token=TGw6jSkV8wtxVMUqNYYe1YdSmkz7AVAq3zckp3_xKN4ol8mx21BzVJCm3sn793M4bKJfjhL03FklGzgV8wWGJsXXrMI&loadFrom=DocumentDeeplink&ts=1398.39)):

Anybody that sees it for the first time, almost everybody is like, "Oh, my God, I can literally just be sent a phishing email. And it's like, my MFA is not there." Well, we got a ton. We had dozens or hundreds of people calling in that wanted to interview Kevin. And they said, "Roger, can you pick it up? You know MFA." I'm like, "Yeah. I've been hacking MFA for my entire career."

Roger Grimes ([23:36](https://www.rev.com/transcript-editor/Edit?token=8aw9xPErx1Fpo97Aj4ezvNs83OMaQKw24hIM2bJgWemT5xOPBSUbHZ817PXJosk19Ly1Rv-qOFsVXeQpedna5Q6e0q0&loadFrom=DocumentDeeplink&ts=1416.98)):

And I was surprised by not only how many reporters, people were saying, "Have you all reported this yet to Microsoft? Have you reported this to MITRE as a common vulnerability exploit?" I'm like, "What are you talking about? He's using a tool that's been around for 10 years. And the exploit he tried, it's been around for 30 years."

Roger Grimes ([23:52](https://www.rev.com/transcript-editor/Edit?token=E9AIS1D0djwpil1sNIZ-KX-GD-noCUHGGbs7EcHFNawVmluixjaDo1getxXPREBfttYoz1t2Wq_Ywj4U9ihAEDtnd_k&loadFrom=DocumentDeeplink&ts=1432.52)):

I was surprised by not only how many newbies didn't know that, but my friends that were 10, 15, 20-year computer security experts were thinking it was something new. So, I was like, "Wow." And I ran into a lot of companies that were like, "We deployed MFA. And we've actually been hacked more. Or cryptocurrency people have said, "We got hacked, and I lost $2 million. I've gone back to password."

Roger Grimes ([24:14](https://www.rev.com/transcript-editor/Edit?token=raYDwlUjGDNrhBoDWl104QjOI8wncU6jJKum29qAo5ThTtmF3UYdTlB0KDEdfrlwPj3NKAofBbMcTcpBK2Cd-eXFDNc&loadFrom=DocumentDeeplink&ts=1454.15)):

So, what I came out with, what I figured out was that people get given an MFA solution to log into the corporate networks, or their bank account, or whatever. And there is this on unearned expectation that they can't be hacked like, this thing, and they're told. Use this so you can't get hacked. So, MFA is a good thing to have, and you should use it where you can in most instances.

Roger Grimes ([24:39](https://www.rev.com/transcript-editor/Edit?token=fPP1MSy48v9qM8a49kywQt3KXVTo6fQh5Bwi9j6YIMYjLTvDZWkL4MCgEIL9hkuj0_fW47FOUjsyhkY7Fk-9_jwN7aM&loadFrom=DocumentDeeplink&ts=1479.81)):

Unfortunately, 98% of the world doesn't use MFA, won't let you use MFA. But it's a good thing to use. But there's a difference between saying MFA significantly reduces some types of authentication attacks, which are just a small part. Remember, I just told you 70%, 90% in social engineering doesn't care about your MFA that much, 20% to 40%, patching. If you don't patch your software, it doesn't care about your MFA.

Roger Grimes ([25:02](https://www.rev.com/transcript-editor/Edit?token=bTQgAFT5BPjSTikip4RBf9lKLEjv8SJragUyDwYiSpcz0VFCksiE6t9aeLjaTDmUxb_8u5Cz_5Rw-zkRACvxzNVpMyI&loadFrom=DocumentDeeplink&ts=1502.29)):

So, the vast majority of hacking doesn't care about your MFA. But MFA will significantly reduce the risk of let's say, phishing, they're trying to get your password. If you don't have a password, they can't phish you out of it. So, there's a difference between saying MFA significantly reduces, significantly from 100% to 1%, many forms of hacking, of authentication hacking.

Roger Grimes ([25:24](https://www.rev.com/transcript-editor/Edit?token=E5anKmJO1i89h5PCKI8div6bjJJMdeC2dtWkU8IgE8qTsg7AzP9GmloGp673Lbq5pEzWWl6X8C8l_-HaG0XnypU9VU0&loadFrom=DocumentDeeplink&ts=1524.82)):

And then, what people feel, which is I've got MFA, and I can't be hacked. And what happens when I talk to people is once the attackers learned that the bank or this person is using a particular type of MFA, they just start creating more focused attacks that work more often. And the end user has not been told that they have to worry about hacking.

Roger Grimes ([25:50](https://www.rev.com/transcript-editor/Edit?token=b_IyEGfxvvCnjW_qncDvsR3cVsAhAzAKhc979fUBHo7L5iggKrxfaQxNf3Kt05K0uSj16UtTNd7NiNDYORbdhgzxd8Q&loadFrom=DocumentDeeplink&ts=1550.2)):

They've been told the exact, the reason why we're making you go through all this extra work is so you won't get hacked. And so, they all of a sudden, don't start paying attention. And the phishing emails don't seem as dangerous. The Kevin Mitnick demo of LinkedIn just shows you, click on a link in an email, and its game over.

Bill Murphy ([26:06](https://www.rev.com/transcript-editor/Edit?token=t8TydUYm2S066VyrDM0hBu2pG5rs_bVkURTf46C691VM64q4QW2Pe3QGIyL04igv9AnLndSmQqqPWQzSp3lZ2dd9t0w&loadFrom=DocumentDeeplink&ts=1566.37)):

And you can bypass your authenticator. So, now, one of the things that I think people are faced with is now, large chunks of the population who are working from home, which means that a lot of the security controls, and the analytics systems, authentication systems now, they're truly cloud based. And then, now people are authenticating, and they're needed to federate identity into either Azure AD or some form of flavor of AD.

Bill Murphy ([26:38](https://www.rev.com/transcript-editor/Edit?token=RBsY0PEJEvXQSq71rU6TShOJ0868Uf9DpQtgJIGpVf4YDhpNgue8MZMyz90W0yGT_oCuiSbjoN915ypMg3AlLa3uywM&loadFrom=DocumentDeeplink&ts=1598.35)):

And now, we're layering multi-factor into that. And sometimes, with third parties that are inheriting Microsoft's, sometimes they're taking over Microsoft from an identity perspective. And I think there's a lot of complexity here. And then, they're going into the apps, and the actual account takeovers are happening, where there is impersonation happening, impersonation attacks. So, I'm just wondering, where do you think we're going with multi-factor now in this world we're in?

Roger Grimes ([27:07](https://www.rev.com/transcript-editor/Edit?token=pl1-Om-oZt6utyA6zjn015RNP7BS7Qk2MTiVbwbDHh6I-bcbCme8imgvIZ83OcXBPxSA9nCtp55rq8oPDaSVayM075E&loadFrom=DocumentDeeplink&ts=1627.87)):

Well, there's certainly more of it. There're going to be more, and more, and more, and I'm big fans of some types. I literally pick winners and losers in the book. I don't like SMS-based multi-factor authentication.

Bill Murphy ([27:18](https://www.rev.com/transcript-editor/Edit?token=vy0AymwIjPWwQB0bJZwTDgS01VHeOdtyPUph55Cc0mc7BAkQHb6ITFWc7Z8xvoI5y4NlhRaIIWQpy2XlRiRkzbkU_zk&loadFrom=DocumentDeeplink&ts=1638.2)):

I know, you don't like it.

Roger Grimes ([27:20](https://www.rev.com/transcript-editor/Edit?token=sA_ZyJGAMYxK1TEOJydZxw1DRpJN9nva-zXqrDQa7FpaXhHH7_0iEUslLW12DYeUbdH3rm6PMN4mYhJMMp9rjK7qgiE&loadFrom=DocumentDeeplink&ts=1640.23)):

I like push applications. So, you've got a phone application like Google, and Microsoft, and others will send you a message. Is this you trying to log on in? Yes. The push applications are fairly secure. Fido things are fairly secure. Fido puts down man-in-the-middle attacks and easy phishing attacks. So, I'm big fan of those two technologies.

Roger Grimes ([27:38](https://www.rev.com/transcript-editor/Edit?token=LGdWKm39sVXyCuVd-auM9bx0FWQxQSVaH-oSZ_rTrIKT_3JVR0z4REyjZ0TALdF3b5T9j6CnqYPV275DCnT4a7RSifI&loadFrom=DocumentDeeplink&ts=1658.82)):

Fido is becoming a bigger standard, but it's been 30 years. I've been waiting for 30 years for some MFA. Back in the day, it was RSA SecurID, if you remember that.

Bill Murphy ([27:51](https://www.rev.com/transcript-editor/Edit?token=ByVLFLOfgBBN1LAEYVc-FbpTyleW6AGEwQFgu7hWJt5LJ0E9l1BXtXEev5QDJpoROvEhJVnREKbJhHo_qZL_-JNYiD8&loadFrom=DocumentDeeplink&ts=1671.39)):

Yeah, yeah. With the tokens, yeah.

Roger Grimes ([27:51](https://www.rev.com/transcript-editor/Edit?token=sfWl3m-Z4QbuA5cEEHL7fJ_z79bP02F9jHrTj50UbKMSV97iNADU9N3gUJVBZw4VfeOSvtmhnO89KP3aH29bfsdrE2U&loadFrom=DocumentDeeplink&ts=1671.86)):

Yeah. But whatever becomes big and we're told is the next greatest standards, right now, let's say it's Fido. And let me say, I am a huge-

Bill Murphy ([28:00](https://www.rev.com/transcript-editor/Edit?token=8GZSnDsHofdceQh8n_qLZeYMf8-6sHraudIirZCK47mcCGi8OBt9k7A5x5Vl_dPXJMydNYVP2qvvUur948jYfRSuJkg&loadFrom=DocumentDeeplink&ts=1680.1)):

Can you explain Fido, just for my semi-tech people that are listening?

Roger Grimes ([28:03](https://www.rev.com/transcript-editor/Edit?token=4ahEBEgOUTgNj85UATIisE_GqC1BJPybdh4OT7fFtIin0z87wENlYexNv2izQwHp6DzIkUuL3kl2Hhnds1ta06F90rQ&loadFrom=DocumentDeeplink&ts=1683.8)):

Yeah. So, Fido, behind the scenes, it's using a public-private key. It's passwordless authentication. Probably the most common types are something like a hardware key that you plug in, a YubiKey or something like that, but it could be biometric or any other. It doesn't have to be multi-factor, but it often is. But the idea, the great thing about Fido that I love is that it registers its token with the actual website, and won't work if you get misdirected to another website.

Roger Grimes ([28:34](https://www.rev.com/transcript-editor/Edit?token=-zGG6btjjxWrk-HrYB9wn6NooFHQmV3TNhJXcNlo6TPC9-av0fSYWrAVJ-JTYOJA0bRChjAFVxBdBcynPZ3KAABBAcc&loadFrom=DocumentDeeplink&ts=1714.42)):

So, there is this registration, where you're taking, you could have a Fido key, or a hardware device, software device that is registered to you. And then, you actually have to, ahead of time, register it for every site and service you want to use it to. And if somebody is trying to misdirect you to those places, it's not going to work. It's not even going to come on. But the problem is okay, I can't hack you that way.

Roger Grimes ([28:58](https://www.rev.com/transcript-editor/Edit?token=m_RFQetqocmQ6r9pYzRNAD8hS6e0Z5nAiiPoRpQf7twYmLF_obUYmi91um3je-zXRCa2nsfnX_BUu6Nv2-gDqyfKvGs&loadFrom=DocumentDeeplink&ts=1738.21)):

I looked at 130 MFA solutions, I can hack them all at least four or five ways. And most of them 11 or 12 ways, and it's funny, the MFA people always are like, "You can hack mine. You can have mine." And then, I just literally look at a solution in five minutes. I'm like, "This is how you do it. Boom, Boom one, two, three, four, five." And they'll come up, and they'll fight me, and in fighting me, I'll find three, or four, or seven.

Roger Grimes ([29:18](https://www.rev.com/transcript-editor/Edit?token=wPpq312A6Pabd876Dzwb34eH3rxlTgz0eRcVJ5nntAQ-_1TR5xu3fP6U34NUhdFFSCREF_DNnH_K9hMz3WEZay2VTCk&loadFrom=DocumentDeeplink&ts=1758.92)):

I have so many people tell me I can't hack their MFA solution, and I can, just verbally in their face, and I now go I want $20,000 before I go through this exercise. I'm just tired of doing it. You need to do some threat modeling on your solution, read my book if you want to. But there is no solution that can't be hacked multiple ways. Because a lot of the ways are even out of the control of the MFA person.

Roger Grimes ([29:41](https://www.rev.com/transcript-editor/Edit?token=O5RhkJtKe0-ZURH41DFRywnqSkfSXiPyfAHxdM4N6X5KtmJQ9BOBPttl9F-bmYAn2qNRq-PBlyxxZ3ZPWGXyGuJt1iI&loadFrom=DocumentDeeplink&ts=1781.91)):

And they'll say, the vendor, and they go, "Well, I can't control DNS, or I can't control this." I'm like, "Of course, and that's why you're hackable." But if an end user is relying upon your solution to make sure that they're not hacked, and they get hacked, they don't really care that you weren't the reason why they were hacked. They just know that they relied upon a device that they told that would allow them not to get hacked, and they got hacked. That's the real world.

Bill Murphy ([30:05](https://www.rev.com/transcript-editor/Edit?token=pHU9PTX1-xaD9UVP9ON9uM31j7sOluWuFfP9bgD8386pTxbu-TOzc9lGDfmiJEeZiTrXGVn_rOvNBKzkhNqlFRTA-Vk&loadFrom=DocumentDeeplink&ts=1805.42)):

Using your 80/20 analysis that we were just talking about earlier, is there some high-risk areas that most CIOs and CSOs that if they can check the boxes on multi-factor authentication that you think fall into that highest risk category area where you got to peel back the onion a bit?

Roger Grimes ([30:25](https://www.rev.com/transcript-editor/Edit?token=eWr8qCHnIsNzriVbG9l4h34EkM0sNr3YCdYmDWRCkoeR38fP_j-H8D6VuA21DSUY5zUz39FZDYGrAcAbMQxdnXzQGNc&loadFrom=DocumentDeeplink&ts=1825.98)):

Yeah. So, I think any of them that allow somebody to be man-in-the-middle, so that would be like the LinkedIn example, if someone can login to a session, but be man-in-the-middle, and not really be... so what happens when you're in a man and middle attack? It's called network session hijacking, is the attacker convinces you to come into a proxy site that is bringing all the information from your intended destination, and brings it to the victim.

Roger Grimes ([30:53](https://www.rev.com/transcript-editor/Edit?token=5uVB0h9tV6kD9wKxzDMe7bIXUR8vSsqEfIdk64mWp4vZkVGaSL3cWF8JNXFxMGEcQlp_KsZU-9DgMkMCU04xKxggDN4&loadFrom=DocumentDeeplink&ts=1853.23)):

And everything the victim says and does is proxy to the destination web server. They don't know there's a man-in-the-middle involved. So, when a solution has that preregistration, where I only work with this particular website, that stops proxies, man-in-the-middle. So, there's a lot of solutions that do that. I like solutions that do one-time based passwords, if it's done well.

Roger Grimes ([31:19](https://www.rev.com/transcript-editor/Edit?token=yjyevwUcStCRg-2gxB8D3bYTkyNy9De2YZMT8GLfqzyQKjSkMOFmxCYxrS6w9F5AUkVzSJJliyQ7gJBX9MTr9_OvJtA&loadFrom=DocumentDeeplink&ts=1879.98)):

That's the problem is that every solution you give me, there's good implementations, bad limitations. Fido. If I see Fido, I like it. But there's Fido one-factor solutions where you just plug it into the computer. Well, that means if you lose your USB key, and somebody else plugs it into their computer, they're you. Oh, it's two factor, you have to push a button.

Roger Grimes ([31:43](https://www.rev.com/transcript-editor/Edit?token=PRlK6lxerAaYplZTrildCipGhKOWmre-CtsbNwVhofHSTR7jCHI7scQo2R4KkqPNFAIMCbeiehipPhrzpv-OWaQiBrU&loadFrom=DocumentDeeplink&ts=1903.23)):

I'm like, "Well, that ain't much of a security bar." Or biometrics, I hate biometrics by themselves. Biometrics can be number one, stolen, and reused, and what are you going to do, change your retina, or your fingerprint? But they're never as accurate as they claim ever, ever, ever. And if you allow biometrics to be used to remotely login like we are in these COVID days, well, you're just being a fool.

Roger Grimes ([32:08](https://www.rev.com/transcript-editor/Edit?token=0a2_LxD7WZTiVCD0eZeAKqephsujrBCrv4cbGahby0KweLbVOSkhcXfJoKRvxPeVHT7EC_SL5QXNJyubLmHaXj6zdJA&loadFrom=DocumentDeeplink&ts=1928.85)):

Because anybody can fake that fingerprint, our biometrics, we can't change our fingerprints. So, bad guy steals our fingerprints, then remotely, you're insane if you allow biometrics, because all the biometric readers are horrible. Your fingerprint is possibly unique in the world. We don't know that for sure. We've not taken everybody's fingerprint is unique in the world.

Roger Grimes ([32:27](https://www.rev.com/transcript-editor/Edit?token=v-8vPQgIb6zQlnLHdms5vKZGULYMLaJneniPn49FzuFX6hZyTVa-z8WEPlKSnWuGRh9tkwgQmtZM3mD6fhE3DykCjCM&loadFrom=DocumentDeeplink&ts=1947.74)):

But the way that that fingerprint is read is maybe different from 15,000 people's fingerprints. It's because the scanners have to intentionally not really work that well. Your cell phone, my cell phone, I opened it up with a fingerprint. When I can't open it right away using my fingerprint, I'm mad. And if it didn't let me in, I would stop using that method or stop using a cell phone.

Roger Grimes ([32:53](https://www.rev.com/transcript-editor/Edit?token=8XEUoDJ7cuJYClb42y8FgYtNfe5OggNi0wGuu_9gZLNPrT5yN_ArRO5tFzPwO4pz-sOjaS8PAZVU6qamR6lWsbV1rRk&loadFrom=DocumentDeeplink&ts=1973.96)):

But I'm amazed sometimes how little of my finger I get on that scanner before it logs me in. So, they literally intentionally detune it. And every time you detune the scanner, the reader, the biometric, and they're like, "Oh, your retina is one in a two, three, and nobody can ever have that. It's just not true. It could be. They don't measure it that way because your fingerprints get little micro abrasions, and cuts, and they bulge.

Roger Grimes ([33:16](https://www.rev.com/transcript-editor/Edit?token=Hix_HNDbLB_35M4ibM_HrtPysguIBBiLLqtD3yyD3533D-6JkH9eswBP72v9rD-x3Cqh3k99x8n883j-OPZQlxU0iJA&loadFrom=DocumentDeeplink&ts=1996.1)):

So, they have to intentionally detune them. I like biometrics if you use it with some other factor, but just doing biometrics, and let me say fingerprints, I've spent a life hacking fingerprint scanners. And sometimes it's as easy as going up to the fingerprint reader if they have the flat glass, and blowing cupped air. And actually, the moisture from my air activates the oils, and logs me in as that person.

Bill Murphy ([33:41](https://www.rev.com/transcript-editor/Edit?token=GsmnWFTk9NQmPa2KfEhzBjjns_sAGbMlf42Zt94lAmYC9yReMstex24dsZ6eHKk8Ep9wlIbSzpuLMkIFcuCRVAmSI_c&loadFrom=DocumentDeeplink&ts=2021.14)):

No way.

Roger Grimes ([33:41](https://www.rev.com/transcript-editor/Edit?token=VZCb8IQLP4o1r_ufGcI0hc4bAGW506ujsDeGjInk14wpj58oef3OIOm-Exae-zdRss3OxEWHc-7idoQQYaCr_Eib_g4&loadFrom=DocumentDeeplink&ts=2021.94)):

I've done it on building entry doors all my life. I don't need special fingerprint spray. I don't have to create a playdough finger, hot air. There's something wrong with the system when my hot air activates your fingerprint oils in the system.

Bill Murphy ([33:56](https://www.rev.com/transcript-editor/Edit?token=JQbAdxBMAhN0vOiQ-QnwIBXz9LZ69pRRhXEljEe_1n-pJaTSMxh-PqBqNpZriLwz9mCFC9MS-_Lnc98K_CnQsTEuY0k&loadFrom=DocumentDeeplink&ts=2036.86)):

How did you start out in computers? What was your first experience with a computer?

Roger Grimes ([34:06](https://www.rev.com/transcript-editor/Edit?token=gxzSeCajwbyiQgoqFS25IsL1NpFdxdvF_-zxixpqsT8WoIbY-eDCjxXGCNGU3uuVOsiJm2SqI_MdGd2hsvpM0i0bpGY&loadFrom=DocumentDeeplink&ts=2046.74)):

Yeah. So, skipping when I got into computers, which was a great story in itself, because I was clueless. But computer security, I actually read a couple of good books, a book from Ross Greenberg, one of the early antivirus makers. And he wrote a book called Flushot, where he invited malware people to attack him. That and the Clifford Stoll's honeypot book. What was that called?

Roger Grimes ([34:31](https://www.rev.com/transcript-editor/Edit?token=W4rX2XBbJ-hW3FkdHRGYsBNwHBMoFQorY0H4WZmtCcShHdJpjHUQyG3NJubgkSzomOFCbl0qvsSn3X1VEx2iBJQDfl0&loadFrom=DocumentDeeplink&ts=2071.7)):

Clifford Stoll, he's famous for his one honeypot book, and it got me to honeypots. And then, I joined the internet. So, I was a CPA, Certified Public Accountant working with county firm. Absolutely the worst CPA you ever met. I never finished a tax return that was ever given to me. When they gave me an audit, I shoved it in the back of my drawer where I knew it would fall behind and go lower.

Roger Grimes ([34:52](https://www.rev.com/transcript-editor/Edit?token=MDbx7FHv0liZW_dWRkzCBFUMeR1wQrFjRkJCHeyW8VZ8KEHHDh2hqgCDjfDHXEFXKH7hlPmbdeDDpMq3ym26G7UQL9U&loadFrom=DocumentDeeplink&ts=2092.69)):

And I couldn't find it, and that was going to be my excuse as to why I hadn't done the audit. So, I apologize to anybody whose taxes I did or audit during that time. But I started reading, and it really caught me. I wanted to fight these hackers, and I joined the fight on that before the internet was around. ARPANET was around. It was called FidoNet in bulletin board systems you had to dial up.

Roger Grimes ([35:12](https://www.rev.com/transcript-editor/Edit?token=Y78vB0QiXKbJdu-oB11pkbxZUm95K3MBnQZV6F3306s52QwMAq6Sy5OsQGyzoXjeR6zloE0cnS99-1DNLcqTbClihwo&loadFrom=DocumentDeeplink&ts=2112.95)):

And I started getting viruses, and I started disassembling them for John McAfee. I joined a group called the PC Antivirus Research Foundation. This is 1987, '89. There're only three or four viruses in the world at the time. The first PC virus is Elk Cloner, written by 15-year-old Richard Skrenta in '85. By the time I got into it there's Pakistani Brain, Stone virus is '85, '86, '87, and really, it just sparked something in me.

Roger Grimes ([35:41](https://www.rev.com/transcript-editor/Edit?token=FWYINFObyRnBOPlv_sD76617FsAsHl_rG5FL2kj9SLxv9hInQJdBgFb_YLlu3Ap7jNv5wfnDatP1bEYKltJe0FPAxE4&loadFrom=DocumentDeeplink&ts=2141.01)):

And I was doing it so much. I was disassembling viruses so much that my wife said, "Why don't you do this for a living?" I was like, "No, I've got my CPA, I'm accounting." But she's like, "You're literally ignoring the family all the time and me." Because she would tell me, "You're not spending time with me." So, I'd spend time with her, fake going to sleep with her, get up, and work all night.

Bill Murphy ([36:00](https://www.rev.com/transcript-editor/Edit?token=Ux-VAupLUSSnGIfGfE4_zlU_QUoXi0fDjmvSKtUwIGz3OIlF0_eLEFaqjKORwX-oQywrCLk3AHw8_b4gapdoXNkwUqs&loadFrom=DocumentDeeplink&ts=2160.93)):

You're just that passionate.

Roger Grimes ([36:03](https://www.rev.com/transcript-editor/Edit?token=IQvupgwj8KbTpp7gY1zcqA2t8Gltg0CwtcaZT2IYzSNdidRYUo3sPfY-AH9OrU9RVK9rXI_SPxviW6_nQntnkE1NXFg&loadFrom=DocumentDeeplink&ts=2163.79)):

Yeah. Why don't you do this for a living? So, I went through a lot of different jobs. But even when I was a VP of IT, I was mostly neglecting every job I ever had to do computer security. It was overwhelming. I was in Newsweek in 1992 when the Michelangelo virus was going off, working with John McAfee at the time. I don't know how I didn't get fired because it's all I cared about.

Roger Grimes ([36:28](https://www.rev.com/transcript-editor/Edit?token=v5A0OWb1kCVUmNw8_X-1MgrdCuLnhkz3nkbeZi6s1jRiFqmuY31SSt_Yk0mOvJziEZn91G3LuXq-hxjvAPZXzuRNrzY&loadFrom=DocumentDeeplink&ts=2188.71)):

I remember one time that I had a news crew coming in from CBS News. And I was a PC network manager or something, network manager. And I remember my CEO, just seeing this news crew going to my office going, "What's going on?" I was talking about viruses. But I finally decided one day, I want to do this full time a bunch of years ago, and I've never looked back.

Roger Grimes ([36:49](https://www.rev.com/transcript-editor/Edit?token=I14or0R9T7zbxHe_F2C6IAbhoO_cJ905KmV7CkSAdX8ziRcz9z483kmK4-jPNjQULJuVCvGiDKx_zxTlNFqqCnn9AOM&loadFrom=DocumentDeeplink&ts=2209.04)):

I remember, although, I laugh because I remember I was telling my wife, I'm like, "Hey, I'm going to quit this VP of IT thing, and I'm just going to do computer security full time." And she's like, "No, no, no. We got to make a living. You got aw wife. You got kids, and the house, and cars and everything." And I remember, I was thinking, "I wonder if this computer security thing is really going to hold out?"

Roger Grimes ([37:08](https://www.rev.com/transcript-editor/Edit?token=s3X_nQ8D4YUlN5Ph65QetYFRlxQFjp41xW5W8Kl5a1BNwKB9S8slsuGGGRjAz0jTVTxEX5OSZcRxzCn76y5WfYRRbGY&loadFrom=DocumentDeeplink&ts=2228.16)):

We're getting better at detecting viruses, and we know how to stop it, you just got to stop social engineering and patching. Certainly, passwords would be gone in a couple of years. We'll figure out how to stop the phishing emails. They're coming up with new protocols. I laugh hysterically because that we were thinking, "Is there going to be enough business there?"

Bill Murphy ([37:28](https://www.rev.com/transcript-editor/Edit?token=ZYMYKxtZe5HOG_lPPLkDqYOvOv7A59P1gVpq4S4WRBtv389PjROL3x5MtlSAHeWUVeTdoSsAGxXRMyjPxV3bavwsbIk&loadFrom=DocumentDeeplink&ts=2248.35)):

Yeah. Is there going to be an industry that emerges from this? Because it wasn't popular. It wasn't popular the days that when you get started when I started RedZone in 2001, we got started as a security vendor. And we started working with credit unions, but-

Roger Grimes ([37:43](https://www.rev.com/transcript-editor/Edit?token=3B02FC-Q3qXynfRqmqqGxv9Ze5X-eGyY-dBGkKMMYghc6uu167W_zf0aLzRlxj-hQR3d5dTl3hhhayK_Wo1ubmHXMHg&loadFrom=DocumentDeeplink&ts=2263.18)):

I remember the worm back then, Code Red.

Bill Murphy ([37:44](https://www.rev.com/transcript-editor/Edit?token=NDhUijmnE42Io556pDjarTDNvKB5kB_nybRtQdR9-V8w_4Kr6mdmoi2s7HbKKNHLs_v-Ax8DadKs4va_B11BMGBAaCM&loadFrom=DocumentDeeplink&ts=2264.86)):

Yeah. Code Red, exactly. But it wasn't popular, it's the only specific industries really cared. In fact, the first CSO, do you know when the first CSO was anointed?

Roger Grimes ([37:55](https://www.rev.com/transcript-editor/Edit?token=_upjsZ8NhEmaOqEKWgiRh6VEp8MQ5D1uwTTUoqtQTASOiw2UYJF4W_eXcCczSAkSXeVE-qDU4w0VQ6LHqhF1egA2GA0&loadFrom=DocumentDeeplink&ts=2275.98)):

No.

Bill Murphy ([37:58](https://www.rev.com/transcript-editor/Edit?token=Tg8Sa8C6RxBkHfU9Cc_dS3Io9lrDX_vqLUti4HGqw9KKdFrEwpLOVTIYzqFSMDYZ-GGTRO2D1eDo2XTZ3jBGtJ-Era8&loadFrom=DocumentDeeplink&ts=2278.34)):

I might be off by a year, but I think it was 1998. The first CIO is '95, CIO. And soon thereafter, a CSO. It might have even been later. That official, Fortune 100 type designation. And so, it's a really relatively new profession in American business. You think of the role of the CFO, how long that's been around, or an operations, or the CEO. But the role of a CSO, the role of a CIO is relatively still a new position.

Bill Murphy ([38:34](https://www.rev.com/transcript-editor/Edit?token=2vHKmrOdejgzzA2OyGR_tqkUvtzylKpB8SV05lPogUqGX3lc_wfBFN1Ye9h4YPNB0MXluzFEwhj5DiPJN4BXKvXOJqA&loadFrom=DocumentDeeplink&ts=2314.56)):

And I think it's further complicated because at least with American business, we have gap accounting principles, we have debits, and credits, and you have a governing body that says, "This is a correct accounting for a business." But we don't really have that for security, do we?

Roger Grimes ([38:50](https://www.rev.com/transcript-editor/Edit?token=7HBvarZKyzDxPSd_N58THgId0W9OZ9lqU3j5_HATVDwqcQplk11q4Kc6BFRfNjKLAQMt1OizZrjEr6anudLsQtu9fbM&loadFrom=DocumentDeeplink&ts=2330.45)):

Yeah. And are you ready for a full circle where it gets really bad? Is that now, compliance wins over security, even when compliance is bad. A great example is password policy.

Bill Murphy ([39:01](https://www.rev.com/transcript-editor/Edit?token=9gLroLJZv5aUzN-iY_FhhMYauk0CoA_y7J7vrfuK7CVeh5HHsHwLDYAYGO9WBlypCUtiYrx7nv6zdjcpB5XsMdGQ_yk&loadFrom=DocumentDeeplink&ts=2341.83)):

Oh, yeah. Tell me about that.

Roger Grimes ([39:05](https://www.rev.com/transcript-editor/Edit?token=zEQuLOghtkzuAUMgX2DJOyACYZRVQHC6EmRSZiCZ78ZXWA9ceLagwojuDuAvx9Wl4IJ_1uWfz6guKXF5yTCIKOCd1WE&loadFrom=DocumentDeeplink&ts=2345.06)):

So, this has always been our password bible, the National Institute of Standards and Technology, and they've been publishing for decades of what's called the password policy, and what's called NIST Special Publication 800-63. And they're the ones that said two decades ago, your password should be long, complex and frequently changed, right?

Bill Murphy ([39:25](https://www.rev.com/transcript-editor/Edit?token=wyinUEI7qzv9NS3g_g0wQ-FO4dcnhGAtFX85VoRrMLSIAoi__TqqGL_6p71bUYD_FHbnxMNMLz-uOthkS1MQ4J6wD9E&loadFrom=DocumentDeeplink&ts=2365.13)):

Yeah.

Roger Grimes ([39:26](https://www.rev.com/transcript-editor/Edit?token=iLQIOZX25FAcovTFcqXZ-iuVmK_YgivfVRrRdlksblG7wolNVpkBn8UkItgnOz-C89Jycssr7DsgGhqK7jDYhtsoCQU&loadFrom=DocumentDeeplink&ts=2366.45)):

You name the regulation, PCI, DSS, Sarbanes-Oxley, NERC, the Microsoft policy, whatever. That's what everybody follows in 20 years. So, then, at around 2016, NIST started doing research, and inviting professors that had done research in password stuff. And they found out that turns out, if your password is long, complex, and has to be changed to preset intervals, that it actually increases the risk to the organization or person that they will be hacked because of that password because of password reuse.

Roger Grimes ([39:58](https://www.rev.com/transcript-editor/Edit?token=4KWUGrTxB-NpTmwMwAbwXg50vvvInJrS7Dnv2jS3xcpj_tXVj9fOY8TixhLqBTE_kCeGSquHVW6HjIX-mBO5Hndr4ng&loadFrom=DocumentDeeplink&ts=2398.49)):

So, it turns out the average person has 170 plus websites and services that they login to in the course of a given year. And they only have three to 19 passwords. Due to no fault of your own, like Facebook got compromised, adobe.com got compromised, got my login name, even password is out there 10 times according to the Have I Been Pwned website by Troy hunt. And it is, and I was like, "I didn't even know these."

Roger Grimes ([40:28](https://www.rev.com/transcript-editor/Edit?token=Gv__agD3a3RUXw_aNBYyBGrKgEAChur5QezXyMIc9WLAvWAku-9aS9GCKTRwjVbdHYqXDpsgiKz5oBq_3qSXo0gS89w&loadFrom=DocumentDeeplink&ts=2428.4)):

I joined Adobe so many years ago, how do I know? I was never notified. I didn't remember them being hacked, but they were, and my password is out there, I've checked. And they're older, but that was the problem is that it was reused, somebody gets it on Adobe is let me go see if Roger logs into Amazon that way, and Instagram, and Facebook. Turns out, there's a really high correlation.

Roger Grimes ([40:49](https://www.rev.com/transcript-editor/Edit?token=ec9GxFZ8Xm4lUDFAlyzpR2Ezkin08uGYfIzTgTCT2xwJa-Ee6JpSBtlZ0qgtT2Zn21iZ6o0kuZFVtnzlUiyz8Ke4b-8&loadFrom=DocumentDeeplink&ts=2449.65)):

So, in 2017, September 2017, NIST said, we were wrong, do the opposite. We now recommend don't require complexity, don't require links, do not do force password changes. Only change it if you have to. Don't use SMS. Don't reuse passwords across different websites. Try to use MFA. Don't use the SMS. And so, it's called Digital Identity Guidelines. So, that's been over three years ago.

Roger Grimes ([41:16](https://www.rev.com/transcript-editor/Edit?token=rXq7Y8a1wPdhqrDNjyH4jZBC5s7R_1ngWLFbGl8Ua-6GpPNndgMVc7jKkVqTyrR3h73u0BI5KjsBzPW2Slny-vIFyz8&loadFrom=DocumentDeeplink&ts=2476.7)):

And to date, there is not a compliance audit law regulation that doesn't require the old method. So, nobody, as far as I know, nobody, even the government can follow NIST's recommendation, because you will fail on audit, and nobody wants to fail a compliance audit. So, everybody's using the method that 20 years of data has shown makes you at higher risk.

Roger Grimes ([41:42](https://www.rev.com/transcript-editor/Edit?token=-2iG4CVX-JFwjcycYjPey2YyvBNHMJ3eAClhMAhz_GPyNUctbsmUY_6aO0ZXtj1Q6_cIrnX3327QRMDl8kH4JJVBd5M&loadFrom=DocumentDeeplink&ts=2502.85)):

And when I tell people this, almost all the better computer security experts do not believe me, because it's just common sense that long, complex, frequently change your password is going to protect you. Well, turns out, that's not what the data shows, or there's a great friend of mine that's over in Microsoft Research. I can't remember his name. I'm terrible with names, Bill.

Roger Grimes ([42:03](https://www.rev.com/transcript-editor/Edit?token=FkC7eEfoW1VN2uE1AtJAF8rbm-43juIGbDAkGRuXQYjmt6lvxTid595hhvcC30NnMo1yNzU3VRCuwHAzsuo6Y9YGpfo&loadFrom=DocumentDeeplink&ts=2523.1)):

But he said you can design a system for six million people, but six million people are going to respond the way that six million people are going to respond. And it may not be the way that you thought, and if that's the case, you need to update your system.

Bill Murphy ([42:19](https://www.rev.com/transcript-editor/Edit?token=Xb_vXT2ogdB7mHtMKq6GnwE8CpiJ60ZS5KrcKe1FBqCnMZHpCAkEdG5fD8TZcNzdS1F3_vbk2fWiwXTjH8VE68T1rZE&loadFrom=DocumentDeeplink&ts=2539.91)):

So, when you look at right now, multi-factor is, what's the message that you want people to take away from this? Because I keep coming back, I interview a lot of CIOs, and it is very complex for them because they're maintaining systems now both On-Prem, some still at their own data center, and Amazon Azure, and then a wide variety of SaaS applications.

Bill Murphy ([42:52](https://www.rev.com/transcript-editor/Edit?token=0x1N8PyLuTyuoPRwCviKNIiSNeDc___FqysaP6lgi9u_JIMIJsHJihYaqPDsWHfUyDTtTYeSqAshtZfQ1xkjumeSFnE&loadFrom=DocumentDeeplink&ts=2572.22)):

And they've got to authenticate people into the systems. And they're not quite sure how to do it. And what I've heard over the past two years is we use Okta, we use Duo, we use Azure AD, and they're hustling. They're hustling their buns off to get the systems installed. And I think they think that they're done. They're complete.

Roger Grimes ([43:15](https://www.rev.com/transcript-editor/Edit?token=dqB1J0ZJljSVryqFXwSL35ILHr30aPkuCg-uwNtb-yfhKR9s8Tg5x1wKYyxnUio3Ww-m-hVJAwr07KJFOAQFzgUHngY&loadFrom=DocumentDeeplink&ts=2595.04)):

And it turns out, it's only reducing risk, probably certainly less than 10% of their overall risk, and probably closer to 2%. But let's say let's go 10%, it's reducing 10% of your risk. So, instead of it being the security panacea, the reality is you just got rid of 10% of your risk. Let's give the maximum possible it can be, you've just nailed 10% of your risk. But what's that mean?

Roger Grimes ([43:41](https://www.rev.com/transcript-editor/Edit?token=h0PaaS-K_XABbYXT17V1B2nUHeuxZsEKBTdu-9d1poTw26bRDvAJA0JDINA4P5vPKagD_QDIDNo1EQ98bnrmLIViCxI&loadFrom=DocumentDeeplink&ts=2621.53)):

That means, well, I need to go find out what that other risk is. And it turns out that if a bad guy can make an end user run a Trojan, hey, here's your new VPN software, we're getting ready to switch VPN software because everybody's at home and been complaining about the Cisco VPN. So, we're going to yada-yada VPN, and you need to run this executable, and put the new VPN.

Roger Grimes ([44:05](https://www.rev.com/transcript-editor/Edit?token=Bf8nLQQeN0hLDuSLR5GvGtnFgK1Uo8L3snqKC1CcgyqmZCPZ4gvmZqNHBWOwtnezcdCwpoHzupgeXQvNk0tWE0-mp3U&loadFrom=DocumentDeeplink&ts=2645.62)):

If you can trick an end user into running an executable, your MFA just doesn't work. If you're not patched, the MFA does not work. And that is 90%. I even say password policy, password policy only helps stop two type of password attacks. There's a lot of password attack types out there. There's account takeover, and there's guessing, and cracking, and all this other stuff.

Roger Grimes ([44:28](https://www.rev.com/transcript-editor/Edit?token=VjIXwyy_tbkAi1f26oP4BDtDByHfsWjV04D3AWpB-4gjKQLbS_E0K7MCOXxjJIQbrwoGDf-M1yCOTLOGA1HyIFacDyQ&loadFrom=DocumentDeeplink&ts=2668.34)):

Password policy only stops password guessing and password cracking. In order for your password not to be guessed, it just needs to maybe be eight characters, and maybe some complexity. You probably don't even need complexity, but add an uppercase or a character. No one is going to guess it. Password cracking, they can crack eight-character passwords now, one person, some guy sitting at home in under 25 minutes, or I'm sorry, under two hours.

Roger Grimes ([44:58](https://www.rev.com/transcript-editor/Edit?token=6t6kwDAsDMkGUdnAY5Yu6s7GUEe9_Q7NHf8anIhkVgKLxK0TnN2sM10eRpiRgnatj4G5l89Gi7dp8Tq1x13Ul--qjFE&loadFrom=DocumentDeeplink&ts=2698.24)):

If they use Cloud computers, four or five Cloud computers, under 12 minutes. Your password is not safe from password hash cracking until you get at least 16 characters. That's what we know about. We know that somebody has cracked up to 15-character passwords publicly, maybe the NSA or China can do more than that, because they now have password hash cracking rates that do 300 billion guesses a second.

Roger Grimes ([45:21](https://www.rev.com/transcript-editor/Edit?token=YrAzXWp9j9eF0oUU6J3xIeIseaPJtKdOlEzq-ZWlWUgIeDgsMesKIQYZy5a64MnPu5_zzqhkSSvYh48SBPcC60EcAuE&loadFrom=DocumentDeeplink&ts=2721.4)):

But this is what I say about password hash cracking, in order for somebody to get your hash, most of the time, they had to be domain admin, administrator, or root. They were already in your system or network with the ultimate king keys of the kingdom. Instead of cracking your hash, they could just keep log you. So, the reality is I'm not that worried about password hash cracking, because it's game over.

Roger Grimes ([45:48](https://www.rev.com/transcript-editor/Edit?token=Q-pnulE_jFWUHBrbULzkQeYORGvWS3le3KPH7DXu2IKcWhIsotaT79MB0Wy6Hvy64bnkT8W2yCDc_YKWb0hgs7ETOc4&loadFrom=DocumentDeeplink&ts=2748.63)):

They're already in. They didn't need to steal your password hash to do what they're going to do. So, it's really password guessing. If your password guessing, your password doesn't have to be that long. Although, I do personally believe that it should be changed at least once a year. So, if it gets hacked, and it's somewhere out there on the internet, the dark web, they're not hacking you seven years later.

Roger Grimes ([46:08](https://www.rev.com/transcript-editor/Edit?token=GZa1V4ATfYj6JGogrvdJrS-xTZWQQR9OETUtSiy2PmmzQuh42ETUPbDeBCb0RgdAKWIfDu9Oejq1EqxnN13m2-ohyg4&loadFrom=DocumentDeeplink&ts=2768.16)):

So, that's my personal thing. So, my personal password policy is use MFA. Use MFA where you can, which it turns out is not most places. Then, you have to use a password. If you have to use a password, try to use a password manager because a password manager allows you to easily use long and complex passwords, which helps stop all of those types of attacks.

Roger Grimes ([46:28](https://www.rev.com/transcript-editor/Edit?token=uarfktHNTGC3zQBaOCQG0FIy277WrosaW9-c0Dkn5cO_xnZJVLTsGGRzodPFX-NTxf8WCUx8pVzGwI08wVrEfhqiVFo&loadFrom=DocumentDeeplink&ts=2788.95)):

And you can use a different password on every website, and all it costs you is a keystroke or something. If you don't have a password manager, I think passphrases. Roger jumped over the dog.

Bill Murphy ([46:39](https://www.rev.com/transcript-editor/Edit?token=LbMWnzwUf6CwWgs6AhHC4BWXq2Nqj6NjeqRylYnd9Vj6kzInbU8FI1jPcK8SnkdFyvrB0mPDKM3rDHV2xswr8GZYwnQ&loadFrom=DocumentDeeplink&ts=2799.47)):

Sure. I was going to ask you about that.

Roger Grimes ([46:41](https://www.rev.com/transcript-editor/Edit?token=wWjibdHo4br2qa1Af1Mezk6iVEUws1CQWCnevEMZ0HK_V11HRgAhDOfQkluSB8EWtxuoRsszgOkvY8hOIkdPse_SwuU&loadFrom=DocumentDeeplink&ts=2801.21)):

Longer is better than complexity, because as soon as you throw complexity into it, the human being if they have to remember it and reuse it, they start to either reuse it on other places, or they start to create patterns. So, it's Roger jumped over the brown dog one, Roger jumped over the brown dog two, Roger run over the brown dog three, and they're using it across the internet.

Roger Grimes ([47:00](https://www.rev.com/transcript-editor/Edit?token=NO5luPFsbnVe4okQv6O5p8vaHyHKYyJyNvMozmAmnD3TOxoJB-R6oBWUe5uoxmzOH8qnWLh6Qcrj6-1q8VXb61ZOFKg&loadFrom=DocumentDeeplink&ts=2820.3)):

And then, when the bad guy finds that, he's like, "Look at this, this is Roger jumped over the brown dog one, and Roger jumped over the brown dog seven. I bet if I try a couple of these numbers on his current account that it's going to work."

Bill Murphy ([47:12](https://www.rev.com/transcript-editor/Edit?token=6OD9BpvohetEHo3lGe3KSs2Kv_cKL6Yjd69uEtaOhHNNgC6kl34pzYgq2tr2-tKC25yF8Z2zPcKO17wdbJtCCEtc2RE&loadFrom=DocumentDeeplink&ts=2832.4)):

Is that where your part of your passion with quantum computing comes in, it's just that new capabilities potentially of cracking passcodes, or does your interest in quantum go beyond that?

Roger Grimes ([47:22](https://www.rev.com/transcript-editor/Edit?token=oZSMjMkE_aIRqijRkPHjUKTLqKE1sAaWGkB8wpZmwUrNeCPJOfdEFay3FSFYxg8iyz30gHiIYwQs6NdkjktqW3xZkH4&loadFrom=DocumentDeeplink&ts=2842.22)):

Yeah. I've been a 30-year quantum physics hobbyist and my brain is always hurt trying to think about it. But certainly, in 1994, Peter Shor came up with an algorithm that's now the famous Shor's algorithm that said, "Hey, if we get quantum computers, and they have 2,000, 4,000, 8,000 bits known as qubits, and we're just getting ready to have in the next year or two, once we get enough quantum..." and back when Peter Shor said this, there was no quantum computers.

Roger Grimes ([47:51](https://www.rev.com/transcript-editor/Edit?token=PgMHjXkdIJID5OC0nV-xHracfAheKwR23HPCF5q2ctBWoeOXxgnKx9xgu2HQbJ-BV6XSR4yJR3OGcyEtFL4mcMgSIHg&loadFrom=DocumentDeeplink&ts=2871.3)):

The first quantum computer got built in 1998, had one qubit, qubit bit. Well, now, we have quantum computers with thousands of qubits, although it's not the right type of quantum computer. But I have a friend that he's told me the quantum computer that's the right type for breaking cryptography, they're going to have thousands within a couple of years.

Roger Grimes ([48:10](https://www.rev.com/transcript-editor/Edit?token=PR8DNcfuXarFMFum6KUbQ3dUZ_5t7FOIlHYgLPSlrfhuG4AEJ7bPq0I7anTTSs5KOqeE7PkID2rC5AK22pLjn1HdYCY&loadFrom=DocumentDeeplink&ts=2890.72)):

He thinks hundreds of thousands within five years. So, we're just getting ready to be on this place where these quantum computers are getting powerful enough. Now, let me say, I think they probably already are. The government has them. They're not telling us. That's the job. There we go. But when they do that, they're going to crack anything that are asymmetric, our traditional asymmetric encryption is going to be broken.

Roger Grimes ([48:30](https://www.rev.com/transcript-editor/Edit?token=F7zZmfSDPo0qb6YKKaSeR-1mk-GusvNEVQr2CPuJKg69Gr47o_s1z_QMyDiVZkkT1aqSy86dCeUBGCifLLPwniMkMvc&loadFrom=DocumentDeeplink&ts=2910.52)):

And it's interesting. So, I've been following this since '94. Now, it's finally happening. So, that's why I wrote the book. But the wild thing is, here's another thing. NIST said three years ago, four years ago, 2016, he said, "Okay, quantum computing, where it can crack the asymmetric encryption is getting right. We don't know when it's going to be. It could be as long as 10 years. But now is the time to prepare."

Roger Grimes ([48:55](https://www.rev.com/transcript-editor/Edit?token=-0WvT1uZC0g-Mv05ek_QSFsbKkkJLij3SYBkwRaYb9DDdLuoS_qUANnk2NQOTe0K9vGfBB0ikGIkg9VcJECJTunkoHI&loadFrom=DocumentDeeplink&ts=2935.21)):

So, NIST told America and the National Institute of Science Academies and everything and NSA said, okay, in 2016, now is the time for every organization to start preparing for this. Yet, I don't talk to anyone that even knows this is an issue. It's like this looming Y2K problem getting ready to come across us. And when I talk to people about this, I gave a lecture on it today, it is astounding.

Roger Grimes ([49:18](https://www.rev.com/transcript-editor/Edit?token=WbaZJMjW8lSf1sJiQPoOoudG3dUNgE-1q65gPIi349NWe-5OqKWcvDx_sOMS4xyXVkqZIxLmr7uRottDapJEmd_laNc&loadFrom=DocumentDeeplink&ts=2958.76)):

People are just like, "I had no idea." And let me say, there are things you need to be doing today. Because if your competitor wants to learn your secrets, I would be sniffing your wireless network today. Knowing that in a couple of years, within two years, three years, we have the quantum computers, I take my competitor's network traffic protected by TLS, or RSA, and I read all the traffic.

Roger Grimes ([49:43](https://www.rev.com/transcript-editor/Edit?token=X5bzZ3vupr0RyOw0Oi9Fj0wnztRrmuaZEiPvQvTO7PeRE4_gn2iOf2xf01G3ipUkfrS4ZYW-VeL6JfceYMhGK3WUnCI&loadFrom=DocumentDeeplink&ts=2983.05)):

A matter of fact, let me say, nation states, if you have to worry about nation states, they would be neglectful not to sniff each other's traffic today.

Bill Murphy ([49:52](https://www.rev.com/transcript-editor/Edit?token=7-xDNXE6aukG9xINXx0W4DcOn3p1ESFFhHPoATnO3038dfIORIO29Xmh68fqGPmRPluAPTutLBSOp9Zq-JSxOmAHrOQ&loadFrom=DocumentDeeplink&ts=2992.08)):

Well, that's the thing right now is that 75% of the internet traffic is SSL. So, a lot of this-

Roger Grimes ([49:59](https://www.rev.com/transcript-editor/Edit?token=DBW-rcw7W2cJ8aK4bfVnYiGWTo2zVJ9rtwHbHpN-Dvk4L8vq-l0M-MUQ69W5eivY_oDaVybun7oymsSGe0MhUsy0IfE&loadFrom=DocumentDeeplink&ts=2999.94)):

TLS, TLS.

Bill Murphy ([49:59](https://www.rev.com/transcript-editor/Edit?token=rxRUMUv15Z5MKUZJG68VyHcAMXTec0MP8oskMhcefgootTLKbPxDjifqi1p4yG3xC3FHwY-DCfDuH5Vd2lVDXGsIh8A&loadFrom=DocumentDeeplink&ts=2999.95)):

Yeah, TLS. And so, in a lot of the security firewalls, and things that we put in place, and manage for people, they're not even putting on internal SSL inspection. So, we're only really looking at web traffic that's up to 25%. They're not even inspecting TLS. But if you can look at inbound and outbound of TLS.

Bill Murphy ([50:22](https://www.rev.com/transcript-editor/Edit?token=J6j4f_6WBp1PAoQr0KozgP8JR4dTIebWovkcZhnUMKmAkT3SVmeFrZvdCk4oAtlQpixMcIDMN-9yzZ_WC2Qjib1o0BM&loadFrom=DocumentDeeplink&ts=3022.03)):

But that means you got to tune certs, and you got to actually do the hard work that gets in way of your end users. And what you're saying is from a nation state level, or from just trying to get advanced knowledge of your competitors, you got to be able to look inside that TLS all the time.

Roger Grimes ([50:40](https://www.rev.com/transcript-editor/Edit?token=xjJBP_8w8gHI5VYk-2qc3JOGw51O3z49E4PTIZSO4clnzYshSS2acM_dCjmSvnlhlg-Y8NO9KI_Oa2H3DdAgdRCmGc0&loadFrom=DocumentDeeplink&ts=3040.69)):

Yeah. If you have a critical secret that you need to protect for five or 10 years, it needs not to be on your network. You need to protect it because the encryption that you... you can encrypt it with symmetric encryption. Quantum computers are going to break the protection of symmetric encryption AES in half.

Roger Grimes ([50:59](https://www.rev.com/transcript-editor/Edit?token=ZtSt2rKxB2UTuc68vuM2e1C_jjij7MZniSmHcZHyUmySAh5W4wGKDzNeoNlJna4XFs-Ex88kEbetCHWuai5OAWorcIc&loadFrom=DocumentDeeplink&ts=3059.66)):

So, as long as you have an AES 256-bit key or better, you're fine. If you have a AES 128-bit, which is very common, that means when quantum computers come, that's a 64. Well, we haven't broken 64-bit key AES, but we have broken 56 keys, 56-bit. So, it's not that far off.

Bill Murphy ([51:18](https://www.rev.com/transcript-editor/Edit?token=m77Zis0gCMCLDIs5nqlCeYuTsWApABRrhoE8IzYELDoUoCFz1-Nr4N-qq8t8zPpeMS6tr-ssKL6mcF5E_7fJiaMhXzA&loadFrom=DocumentDeeplink&ts=3078.98)):

Sure, certainly.

Roger Grimes ([51:20](https://www.rev.com/transcript-editor/Edit?token=mZI0QZQtNJM_P8PQQ7Ys5qY2kjwxu12RuaKGOWflvGxzux6LrX4LMGok5WenUw3uN5uO7umJe9kza9Zmnf1rxMd5d1E&loadFrom=DocumentDeeplink&ts=3080.32)):

Yeah. So, NSA says you should be 192. And they're like, "192, it gets you a couple of years. Who wants to upgrade their ciphers for a couple of years? Just go to 256." As far as we know, unless a new Peter Shor's algorithm is invented one day, and one day, it will be. But for right now, for the foreseeable future, if you have a AES 256, that's strong enough. Now, on the asymmetric side.

Roger Grimes ([51:44](https://www.rev.com/transcript-editor/Edit?token=_6OTecocScT2ryXwRGIPFzy2sBHo2GmSMYW53hXkJxP7fADj7Os6CeT2lhHB-rat68lIN7jf4y5OUpB4bMkIc4l4FIQ&loadFrom=DocumentDeeplink&ts=3104.43)):

So, that's RSA Diffie-Hellman, elliptical curve cryptography, the Fido keys that I told you I love, it's all based upon that. Well, once they get enough qubits, which is very close, if not already done, all of that instantly becomes not protective. So, if you've got a critical secret that you need to protect for the next five or 10 years, don't put it across your network, or you need to use quantum key distribution that is able to securely transport keys that are not quantum susceptible.

Roger Grimes ([52:13](https://www.rev.com/transcript-editor/Edit?token=Cc9WjFE_wuxTHbGhFjr9lt_q6Wa36ltS2imogzxRJLrT9P5XtXSXSupwP-x15PaqY26U07WBJzgREfDL4ARmAl-H0Og&loadFrom=DocumentDeeplink&ts=3133.34)):

And let me say, they've been selling quantum key distribution machines for two decades. The first one came out in 2000. And let me keep talking just one more second here. I think every company, every CSO today, there's no doubt in my mind, per this quantum problem, should be doing a data protection inventory.

Roger Grimes ([52:31](https://www.rev.com/transcript-editor/Edit?token=4gbcc4RiORYiojP5uL9WVgrUdh9x7YpPkKwvEVhMUklTgAo0hIO6x8xixjTkAjqzt-VrfuY9AzjXpp7ir3Eqc2QmT9g&loadFrom=DocumentDeeplink&ts=3151.79)):

Figure out what data that you need to protect longer than a couple of years, where it is, how it stored, figure out what ciphers, what types of ciphers are protecting that data, what are the key sizes. Because you're going to very soon be asked to upgrade all of the quantum susceptible ciphers to what's known as post quantum cryptography, the cryptography that the NSA chooses, because it's not susceptible to quantum computers.

Roger Grimes ([52:58](https://www.rev.com/transcript-editor/Edit?token=z7sgoQBQqlstXlf_YqUYLaBe7-JDJDA0JLXkcMHHvmsCABb1e2bGYpjZEEH7zsgsp70ztj87A0-cAZAD0oMJe752cPA&loadFrom=DocumentDeeplink&ts=3178.55)):

Within the next couple years, you're going to be told to do this massive upgrade. And you need to get on the start of doing a data protection inventory to see how big of a problem, and what you need to upgrade, and where it's located. You need to start talking to your vendors going, "Hey, I heard this crazy loon was talking about this coming quantum crypto break, what are you doing to prepare for it?"

Roger Grimes ([53:18](https://www.rev.com/transcript-editor/Edit?token=Hw3gNvWyVkXC4eqtHdcpaHu8wVxkueu7nEr-QPi3xcAYjIgNHzGSGVugxpRokunhwtPMXRUlESfsMLhymROAlTxOPZs&loadFrom=DocumentDeeplink&ts=3198.07)):

And you're going to hear most people like, "Huh?" They don't know. And it's funny, because the NSA said in 2016, you need to start preparing now. And this is what they meant. Also, you need to create policies so that people aren't buying systems that are bringing in weak crypto today. If we know that AES 128 is too weak, I need to make a policy saying we're not allowing anything in unless it's AES 256. You need to stop the hemorrhage of what you're going to have to upgrade in a couple of... well, it could happen at any time, up to a couple of years.

Bill Murphy ([53:49](https://www.rev.com/transcript-editor/Edit?token=ECuiyfvqW6UFc7egAcfMY0uvc4vdPBo3vddKIT_hetasDNfBt83Xs06gli0vnEYCRNOUEBtE0XP_z_b3fzKUQ0SHreg&loadFrom=DocumentDeeplink&ts=3229.83)):

That's unbelievable. I love it. It's just so key to the future is the quantum capabilities. This is going to give us a lot of the positive benefits from if you consider AI, and machine learning, some of those things positive, but it's also going to cause some of the swing the other way.

Roger Grimes ([54:08](https://www.rev.com/transcript-editor/Edit?token=CO5bswe5rfH5d2IpgSKY5mdIUKGX0santPfSu10Me-QDg__Tnz3x79DHW8Rdj-zdeP4QodOt--UDSTETJe8H-GmmTRo&loadFrom=DocumentDeeplink&ts=3248.82)):

Yeah. I think quantum computers are going to give us things that are more life changing than what the internet gave us.

Bill Murphy ([54:15](https://www.rev.com/transcript-editor/Edit?token=yGYBXyohZv-8uX7d-0ii3SMJ6lmN7Y8G2qMAz2Zhz_Uym2b5jmAxlJ5U2g0pT9o1ApjCHsOC2tgwmMySBM6-gBczA1Q&loadFrom=DocumentDeeplink&ts=3255.98)):

Yeah, for sure.

Roger Grimes ([54:17](https://www.rev.com/transcript-editor/Edit?token=qZeTjkxPZqNIlEikLRP_8wuivinfk5_Hz6LMRFsSdd9uONA3U2hsR-Lqv2FoPRwFil-3urf64E6QZDetnXQFqQZ5Q3E&loadFrom=DocumentDeeplink&ts=3257.6)):

And I think about you and I, we were around before the internet, and we're like, "Oh my God, we can do so much today." I think quantum computers is going to be even more than that, which is hard to conceive.

Bill Murphy ([54:27](https://www.rev.com/transcript-editor/Edit?token=FT4d9T8hF_Okl2GMDlpnDo8ZLwdcfGz5nwFeJWOxdReD1-WXUd1janNLFGqwqd4EEw-oOid5aFclGfGsoNZnJ1hpjBk&loadFrom=DocumentDeeplink&ts=3267.76)):

Well, right now, with the current chipsets, we can't get to the next level without burning... we're right at that cusp of the chip manufacturers right at that top threshold. So, quantum is going to allow that-

Roger Grimes ([54:39](https://www.rev.com/transcript-editor/Edit?token=EdT2eyF54FdYo9DvxXLfIdNkJ-LIek2TS_cZfqnudSoV2xQ7x7-XnkFuizuEcg8pU-VkV95yk6rY59zOmxEnPkyqqss&loadFrom=DocumentDeeplink&ts=3279.57)):

Bill, I've been hearing that since probably eight megahertz. I hear that. I've read that story 20 times. And then, all of a sudden, Intel or AMD, or somebody figures out some, I have heard that threshold. They're like, "Oh, we learned that we can use cadmium atoms." And yes, the wild thing about quantum is that it doesn't have to follow Moore's Law. It seems to be following Moore's law.

Roger Grimes ([55:05](https://www.rev.com/transcript-editor/Edit?token=TdZlrcMaSYKuEyHjycqWn7uvd7wZ4SRL0hSZolZnsVcRgV8Pri46KHR7TpnvP1_rhVounPXLr6G6d7KNLJYMyu03zM8&loadFrom=DocumentDeeplink&ts=3305.97)):

But you get exponential, so every qubit in a binary computer, if I have one bit, it can be one or zero, but it can only be a one or a zero when storing or transmitting information. If I have two bits, that's two ones or zeros, but it can represent four pieces of information, 11001001. But it can only be two bits of information anytime it's transmitting and storing information.

Roger Grimes ([55:29](https://www.rev.com/transcript-editor/Edit?token=oy-bnAntk1AgCmUYJr2XV-Fp2kEbMcHtNomdJvkPJa0iB_b8vmz55IR1zYJ9sqG7PHYmdGJa8YFdJGTrUWTJpovYplI&loadFrom=DocumentDeeplink&ts=3329.37)):

A single qubit quantum bit can be three things all at once. It can be a 01, and a one and a zero. So, as you start to add cubits up, let me blow your mind here. They think that they can fit all information that has ever occurred in the universe, every atom molecule spin, recording of every atom move in 400 qubits. And I just told you, a friend says like, "We're going to have a couple thousand within a couple of years, and hundreds of thousands a couple years after that."

Roger Grimes ([55:59](https://www.rev.com/transcript-editor/Edit?token=vtoz9P89NDMo4Kw16QUDrENyAX63OA4ndoRDcjLYXLOqVnSSTeWhnMka9W9lyTUtpp4MSSiQPKoY7VpFcGiU9E7h76o&loadFrom=DocumentDeeplink&ts=3359.68)):

We're going to have this incredible capacity that they're going to be making better medicines, better car batteries. We're going to be able to drive our self-driving cars without having stop lights, and stop signs because we'll figure out how to adjust the speed so we keep moving. Our medicines will have less side effects. Every time I hear a medicine commercial today, it sounds like an SNL parody commercial.

Roger Grimes ([56:20](https://www.rev.com/transcript-editor/Edit?token=4dHjCWP7oB05FgN8Kuh5oTlj-ea7yxOtbZztrUEUb6_Pwams_QUzskbwamJ5rGIuKqxI1wVEIbcJEzR3hZ94Jd4k4-o&loadFrom=DocumentDeeplink&ts=3380.07)):

And in real life, they all may cause diarrhea or death. And I was like, "Well, why did you have to put the diarrhea one because that's the last one that's really captured my attention." This medicine calms you down, but may cause homicidal thoughts. I'm like, "I don't think they had to print it unless it was really seemed to be indicative of the medication." It seems to me stop. The trial didn't fail.

Roger Grimes ([56:41](https://www.rev.com/transcript-editor/Edit?token=68xSPnFGSP5L-go1YejzNKIcnCF5FmbuiPhx06_qxkmxqze15kQWdLrPAYU4CtLXm-E3713a1EtNWbJDfoQs17RLPnM&loadFrom=DocumentDeeplink&ts=3401.28)):

Somebody was trying to kill somebody, because your medicine, they didn't fail. But hopefully, the quantum mechanics will allow it to be more successful and have less side effects.

Bill Murphy ([56:50](https://www.rev.com/transcript-editor/Edit?token=B7t2UgdujN5T0KYZuF4eRQmgdguR2ZF5XEGgmrWH37lv3Ke-hb1SMgyQO_c6UAJQUswHQXozbgF0wmTf4o4ydTYiC7Y&loadFrom=DocumentDeeplink&ts=3410.87)):

Roger, I think we got to wrap up. I want to get you off to your next webinar that you said you're going to do. But before you go, so your book is out. And it's Hacking Multifactor Authentication. So, I'll put links to it for people to go buy that on Amazon. And is there anything that your subconscious said, "You know what, I got to tell Bill's audience this before I go," or do you feel like you've covered all topics ever for the end of time? Somehow, I don't think so.

Roger Grimes ([57:23](https://www.rev.com/transcript-editor/Edit?token=jeoyfvGYpRiN3V9i0H-pfxg3TtNTWHR2a9NsSLCXFh8qP9s6cZN1Tu06gKJ6_QEh2hIvC1IuCqd04-JYlbPt-MfUsGI&loadFrom=DocumentDeeplink&ts=3443.98)):

I did cover a lot of stuff. So, I appreciate you putting up with me. But just on the multi-factor thing, I'll say that I do cover not only the good and bad multi-factor. But there's no such thing as the right solution for anyone. But I do have in there, I think a really good framework of how you choose the right solution for you or your company.

Roger Grimes ([57:40](https://www.rev.com/transcript-editor/Edit?token=pZzVZ781Tc2EWHgl5n-b_3luAE8DRmHfBeiFrg9z2LZ0E-D2L7SJuZmr_b503J4LHOPaaJTn9JOS6dF7ZR4CdolLxrA&loadFrom=DocumentDeeplink&ts=3460.69)):

Because there's a lot to think of, and I literally have spreadsheets, and stuff, and I say here's the critical stuff you have to ask yourself. This is the optional stuff. One of the first thing is, is what are you trying to protect? You have to pick an MFA solution that protects the stuff you're trying to protect. And no MFA solution covers everything.

Roger Grimes ([57:57](https://www.rev.com/transcript-editor/Edit?token=HT2UE9dQJUdhZhcWVc-ldO3mZFQyy3eqMJh-k2SdyvFDOp6LvHl-OJhCAj8qyLYsVMXhHtmAgVDjSl0DU92VWE9_2fY&loadFrom=DocumentDeeplink&ts=3477.98)):

So, you have to start to pick, "Okay, what am I really going to cover versus not cover?" Because that is the first step and determine, "Okay, can I get Google Authenticator, or RSA key, or a Fido key?" You can't even choose that option until you at least find out, "Well, what do they even cover?"

Bill Murphy ([58:13](https://www.rev.com/transcript-editor/Edit?token=YNHo80bd-l-CkukudDKq-lSRB-xxl6M5_QqJBcwAdqsZLR1Qy3wM_kwXHS4-RUX8wrPdanDD0xAIAus_yxIoRAzi174&loadFrom=DocumentDeeplink&ts=3493.03)):

Absolutely. Well, I highly recommend the book and Roger, this has been a pleasure. It's been a lot of fun talking to you. And I love wide ranging conversations, and ultimately, I really did enjoy the book as well. And so, until next time, we will do a round two sometime in the future.

Roger Grimes ([58:31](https://www.rev.com/transcript-editor/Edit?token=5dtSQvngw9xbL0a24OLNS8KB4FeC52Ge-1_m1WcfYhacwJtgUAszmCQwEXaqXG75mfg5JpB0J59y9ijDh0QhUfa-V4Q&loadFrom=DocumentDeeplink&ts=3511.41)):

Thanks, Bill. Appreciate-

Bill Murphy ([58:32](https://www.rev.com/transcript-editor/Edit?token=7bLZ-Xscxzq0K4qmSLmN7nw9xsjTkMBShIru14ML9ruoCvhmDxQI_eSuS2ZMhOEJKs-WFA0BcRHeWEa51Lv6d6Xfo38&loadFrom=DocumentDeeplink&ts=3512.35)):

Okay. Take care, Roger. Bye-bye.

Roger Grimes ([58:33](https://www.rev.com/transcript-editor/Edit?token=mjheJHc0tzvNtH96C6aNRycKyArNOzUF3c8X53cBMHnrsIMI20IKs71czlnXzlmNL6MwB3DL744KexxVu2iekseTyFU&loadFrom=DocumentDeeplink&ts=3513.3)):

Take care, everyone.

Bill Murphy ([58:33](https://www.rev.com/transcript-editor/Edit?token=op5XbS9QO4plkFWMAr3e7sF401_Kxum5XiPiKpqR2n7CPiIYbN47EfpjApnoQ0NvhS_VuuRVyXLQfQJwyNaSsVY1lxw&loadFrom=DocumentDeeplink&ts=3513.84)):

All right.