FEDERAL TECH PODCAST

Ep. 103 Effective data management at end of lifecycle and after a breach

00:07
John Gilroy from the frill tech Podcast. Today we're going to talk about data volume and emerging time. So, again Hey, John Gilroy today. In the next 30 minutes, you're gonna learn everything you need to know about emerging technologies. And that's it. That's it data. Okay, here we go. Hey, this is John Gilroy. In the next 30 minutes, you're gonna learn everything you need to know about data volume and emerging technologies hit the music Mani. Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Today, we have Maurice Uonuma. And he is with a company called Blanco Blan co Blanco Technology Group, and we're going to talk about a new topic for me. This is about, you know, erasing hard drives and making data secure. And what are the processes involved this standards for erasure why my listeners should even consider it. And before we begin, Maurice wants to tell us a little about your background. And let's jump right in this whole topic of volumes and erasure and all kinds of issues is brings up.

01:13
Yes, certainly. Hi, John. Thanks for having me. Great to be here. So brief background so I'm currently the vice president general manager for the Americas at Blonko technology group. I've been here with the company a little over a year. Most of my background in cybersecurity. Previously with security software company tripwire is VP of federal and enterprise. I've also spent time at the Center for Internet security focused on cybersecurity standards and best practices with a background in IT services, as well as a military background. So began my career as a Marine Corps officer following my graduation from the US Naval Academy served in a variety infantry and special operations roles before transitioning into the very different world of it.

01:56
No worries, I've been up to NIST many, many times the Washington DC area and talked to a lot of people. Certainly I've referred to NIST standards over the last 15 years, but never, never in the last 1000 interviews, have I talked about NIST standards? For erasing I just, it's brand new topic to me. Why is this becoming a trending topic? Why is all of a sudden more and more popular?

02:18
Yeah, that's a great question. I think you're referring specifically to the NIST Special Publication 800 Dash 88 standards for media standardization. And these are the technical standards by which a various different types of devices can be erased in such a manner that the data is unrecoverable in the future. There are different levels of it NIST clear a racist, permanently irrecoverably old data that is accessible to the end user, the purge standard is the sort of highest level of data erasure, and that actually calls for accessing parts of a drive that are not typically accessible to the end user. So the significance of that is that it will erase a device or drive a computing device of some kind to a standard, whereby the data is not recoverable even in a forensic laboratory.

03:12
So the scenario is this. Let's say I'm working for ABC agency, and I have some storage in Google. And then I decide is too expensive, and I want to go to AWS. And so I move everything AWS. And so my question is, well, what about that stuff that said Google, right. Is that a question people ask is that what's up with consideration?

03:33
It is it is a question that people ask, typically, in the case of a cloud service provider, how that data is erased is tied in with their service level agreements, as you can imagine, so a lot of that for the end customer, right federal agency, large enterprise where even an individual is based on those contractual requirements. But regardless of who calls for it, and what the standard is, at some point, some storage media will typically need to be erased and erased in a manner that is compliant with a variety of different standards and requirements. So there are of course, security and privacy requirements, I call for that there are concerns about data security, in general and confidentiality that also call for that. And so typically, the organizations who are handling in most cases, the underlying hardware, so the servers, the storage devices, as well as laptops and mobile devices are all sort of fall within this realm. There is a need there comes a time, typically at the assets end of life, when permanent Data erasure is called for. Now, there are also times throughout the lifecycle of the asset when the asset is saved being redeployed, meaning that an employee departs and that laptop is erased and then re assigned to somebody else with a new image on it. There may be another scenario as well.

04:51
Well, I've certainly have used the phrase software development lifecycle SDLC we all know this one, but I never thought of this part of a lifecycle. even talks about, you know, maintaining the code and patching it and making sure it's secure. But what about the end of the lifecycle? What happens when Gilroy software gets replaced by some better product, Maury software or something? And so, is this part of a regular checklist that the dev SEC ops people have when they transition away from an app?

05:18
I would say yes to your question about is this something that's considered that the assets end of life typically, it's not the dev SEC ops folks, typically, it's the IT asset managers. Ah, so it's it will fall into different realms right. Now, there is, of course, a data security concern here as well that the InfoSec cybersecurity people will be concerned with. And they will be ensuring that the ITSM managers are in fact ensuring proper chain of custody and certified ratio with audit ready evidence to ensure that's been erased. But typically, at an assets end of life, particularly in an enterprise or federal agency scenario, the device will either be physically shredded and destroyed, or it will be re used, recycled, repurposed. And there's a whole industry called iPads, IPS, a disposition firms that will essentially TAKE IT assets at end of life from an enterprise or agency customer. And they will do a variety of different things, but that essentially what they're trying to do is recover value. And whether that value could be recovered by reselling the device, sort of complete, and it's in good enough condition to be resold into the secondary market, which is a booming market, or it may be harvested for parts. So they may determine that some parts of that device are reusable, they may be harvested for recycled material, like the actual raw material, right that is being used to produce these devices. And then there are other scenarios where the iPad is obligated contractually to physically shred and destroy the device. And sometimes

that is because they cannot recover sufficient value from the device. So it's not worth it to them to try to harvest or resell or recycle. Or because the customer essentially demands that it be physically destroyed.

07:09
Well, I think this certificate verification, I think this will be an important to have, because I would think it would be can be loosely applied. Let's say.

07:19
That's a great point, John. And that's that's where we see there, you know, the actual technology to do a ratio to a NIST standard or some other standard there are, there are multiple different standards. But NIST is arguably the industry standard these days. That can be performed a number of different ways, but it's to do proper data sanitization is really three parts, you need to thoroughly erase to a standard, like NIST 888, you need to verify that the erasure has been done for your own peace of mind, if you will, and then you need to be able to provide evidence that's been done, so that you can prove it, you can prove it to auditors, you can prove it to your management, you can prove it to citizens and consumers. And so those three parts are essential for complete data standardization program.

08:08
Well, you got a military background. So you probably understand the logic here. I mean, so the NIST has a standard and the DOD has the standard, as to two Oh, point two, two, something like that. So similar parallel how they differ.

08:23
There's been an evolution of of standards over time, the DOD, standard 5220 Is this commonly referred to Yep, has been around for some time. The NIST standard has arguably become the de facto standard. And in fact, there's a brand new one I say brand new is within the last year or so from I triple E. And 2883 is the is the number associated with that standard that is similar to NIST in the sense that it addresses media standardization, but takes into account some of the newer technologies, right, so as storage technology has continued to develop in advance, the amount of data that can be stored on a tiny tiny fragment of a solid state drive, for example, is much higher. And the various different means and mechanisms by which that data is accessible on storage media has also evolved. And so I tripoli is now taking into account some of those developments, it may emerge in the future as more of the default standard for now, NIST remains King.

09:26
I'm gonna give you a baby example. And you can apply it to the federal government. So the baby example is, Gilroy donuts gets hit by ransomware. And I go, Hey, I got backups. And I plug the backups in. And then malicious code is still there. And I get hit again for double that amount. And so the issue is, what is what's valid, what's not valid, so use the word data sanitization, I would think that after an organization, whether it's Gilroy donuts, or the DoD or NIH when they get hit, there's got to be a concern. About centralization with what what really happened? Okay, so we stopped the malicious code. Well, what happened in there? And is this a question that comes up in your world?

10:08

That's a, that's a great question. And it touches on where and how data sanitization can be applied in a cybersecurity context. So for much of the past 15 minutes or so, 1015 minutes, we've been talking about sanitary data standardization that is tied, essentially to the underlying physical infrastructure or hardware assets, right, we've been talking about servers, storage, media, loose drives, laptops, phones, and so forth. But there is increasing interest and use cases related to erasure in what we could call sort of live data environments. So it has to do with the data lifecycle management. So that's another life cycle to keep track of. And in cybersecurity use cases, and what you're referring to is a scenario where, as part of a post to breach post incident cleanup, the agency in this case, will want to know that before they reimage and re reuse the infrastructure that had been affected. They want to make sure they're starting with a clean slate. And so running a complete thorough two standard data standardization, could very well be a way to achieve that peace of mind before the reemerging and reuse happens.

11:23
There is a podcast in town called Feds at the edge, and the talk about edge computing. And all of a sudden you think about the incident Ohio, the sensors on railroads, their sensors, the ocean, their sensors, and satellite sensors everywhere. And increasingly, people are talking about computing at the edge. And so compute and store, whoa, all of a sudden, it's not just a mobile phone or an iPad, it's it's some computing service, maybe in a satellite is, is that a concern, this whole computing data store at the edge,

11:53
it is a concern. What's happening here is this is within the context of an explosion in data volume in general. So the amount of data created globally is on an exponential increase that I think is intuitively obvious to everyone. But we're talking about an incredible amount of data. And that data, by the way, is, is not just you know, personal YouTube videos and cat videos on the internet and online gaming, the enterprise data sphere, right? The organizational data sphere is actually growing at twice the consumer data sphere. So as much as we are creating our own data, as individuals, enterprises are creating a much faster in fact, I saw a quote from this is a several years ago, but the Federal CIO at the time says that Kant was referring to the Department of Commerce generating 20 terabytes of new data every day. I don't have a way to verify that, obviously. But if you think about what organizations are doing every day and creating data, now machines are creating data. And we can, of course, talk about artificial intelligence as well, right, where it's generating its own new, unique data, that data has to go somewhere, that data has to be protected. And within that context, is what I think you're referring to, which is Internet of Things, it's devices that are sensors that are kind of dumb in the sense that they're just capturing an input and passing it over the wire back. But there's also local local storage and computing, if we think about set top boxes that we think about gaming consoles, right, for example, could capture personally identifiable information, which is protected as we know. And so from a security and privacy standpoint, how do we address those so as Blonko, as you can imagine, we're right in the in the thick of that, looking at different ways to apply standards like NIST, two new types of devices.

13:42
That make sense. I am not going to name any names here. But there was a incident with a certain political person while back where this person had stuff on a hard drive. And this person used bleach bit. And well, I thought that's kind of maybe that's a precursor this discussion today of oh really what's going on here. And so is it says this is a commercial application or what exactly is bleeding is a temporary thing.

14:07
So there are there are a number of file eraser or drive erasing type technologies out there have varying degrees of maturity, varying degrees of adherence to standard and varying degrees of verifiability and prove ability. And so what I would recommend without naming products either is make sure that you use a product that can meet the three standards, or the three sort of key components I mentioned earlier. It can erase to a standard like NIST 800 Dash eight or I triple E 2083. It can be it can verify so it can go back and double check that it is working. And that number three that there is a a certificate of eraser, preferably a digitally signed hard to modify, immutable record you that demonstrates that that particular drive or device has been permanently erased as of that moment.

15:08
When you said they were erased, I thought of a whiteboard. I used to work with software developers all the time, we'd have when they weren't arguing about hot sauce, food, talking about code unemployment, and we didn't whiteboard, we draw things out and everything else. And, you know, maybe we were had a colo facility. It was early days of the cloud. But But today, if I was sitting in the room with you with a whiteboard, there's hybrid systems, there's dedicated as public cloud, there's, I don't know, where's the stuff stored, Maurice? Well, let's get the whiteboard, it's gonna change. So I think just knowing where the data is, is step one, and then, you know, it could be varying levels of compliance with different storage areas. This is this is more than just a whiteboard solution, I think.

15:53
Very true. And you use the phrase, you know, where is the data and sort of hinting at the the difficulties in keeping track of it. And so I would suggest, right, that beyond the need for effective data erasure, effective data standardization, is the need to have a really solid data governance program in place in the first place. And so this is about, of course, managing data, it's also about protecting the data. So now we're talking about sort of other controls and processes, right? Data Governance is only possible, really, if you're able to classify the data properly, ideally, at the time of creation, because going back and trying to figure out what the data classification should be, there are tools that can help do that. But it's tricky, as we know. And then making sure that it's properly protected based on its level of sensitivity. So obviously, classified sensitive, protected data needs to have loads of protection protection, that are higher than more sort of routine, routine data. But all of that is, is being stored somewhere it needs to be tracked, it needs to be properly disposed of at the at the date at the end of the data lifecycle. Right when the data

17:08
is needed. Yeah. Better than software. Yeah. Does lifecycle That's good. Good. Yeah. Okay, let's go back to Gilroy donuts. So Gilroy donuts gets me pretty big. We got five states with selling donuts we bring in Gartner consultant. And inevitably, when they give me the deliverable is going to be best practice. Well, the best practice here Marie's, and the best practice here is on so so what about best practice for good data management? Mean? Are there guidelines for that? I mean, can your organization provide guidelines.

17:38

So we, if you're referring to the organization, if you're referring to Blonko, I would say we have stayed true to our core competency, we focused on the data standardization part. We also do some device diagnostics, by the way, since many of our customers are not only enterprises and federal agencies, but also the iPads that are referred to earlier, and mobile device processors that are taking our trade in phones and cleaning them up and moving them on to the secondary market. But But we, as you might imagine, have these types of conversations with our customers routinely. And we have partnerships, I'll keep it vague at the moment with other organizations that are a part of other parts of the data management ecosystem. So if you think about the ability, for example, to properly classify or discover data, and that process includes identifying and highlighting the location of sensitive data that has now reached its end of life, so let's say files that have been preserved because of a legal hold, or must be preserved for a certain amount of time due to HIPAA regulations, right health records, but now, as soon as the calendar rolls one more day, now you have, essentially, you're liable for protecting data that you no longer need to keep. And in fact, you're required, in some cases to destroy. And so you go from having to protect it and keep it alive to having to make sure that it's gone in essentially in a second. And so being able to do that properly and and be able to prove that it's been done is a key part of this whole process. So if you think about the whole data management data governance process, data sanitization used to be right there alongside proper data classification, data discovery, as well as data security controls, right encryption, for example, is arguably the primary most sort of fundamental data security control we have today. There are some interesting future scenarios where that may become less viable. But for now, being able to tie that all together in a coherent way for the organization is is really the trick and of course, there are best practice standards. I would point back to NIST I would of course point to the Center for Internet security. critical security controls are some of the places to start.

19:52
Your company is BLANC co.com And was there this morning I saw all kinds of AI never thought of being able to remotely erase data from maybe an employee's old John Gilroy, I got a fire one of my people in the donut shop, and they walked out with a company phone. So you can remotely erase data. Well, that's that's kind of comforting, isn't it?

20:18
It is, it's comforting, especially for enterprise security folks. Right. And so maybe not for the employee,

20:24
not for Gilroy donut, but maybe for NIH.

20:28
Right? That's right. And in an era of, of course, remote work, particularly post post COVID pandemic, in 2020, when we sort of all scattered back to our homes, that has become a major use case for our customers, actually. So it's not just the data center environment, it's also the end user compute environment. It's my laptop here, it's my mobile device that the company may have issued to me. And so rather than the enterprise ITSM manager or security team having to then ask for the employee to ship it back to some office where then they have to go in there and do all this or pass it on to an iPad. to process it. There are ways to remotely either completely erase all of the data on the device, or select files and folders and virtual machines even and so you can be fairly selective about it as the enterprise or you can be very thorough about it depending on the use case, right? So if

it is a employee exit, and rehire, then, of course, you might want to remotely erase the laptop completely, and then have them ship it back. And then you're less concerned, by the way about that chain of custody and what what's happening to all the data on the devices is being shipped around. Or it may be a case where the enterprise says, you know, we want to make sure that we are reducing our data attack surface, if you will. And so we are going to install a file erasure capability, whereby certain types of files or the trash bin or recycle bin, for example, or temp files, are completely certifiably erased, on some sort of schedule or at some sort of prompt like a restart. And that can be deployed as well. So that just sort of being improves the, the enterprise's ability to manage the risk of data leakage, and data spillage?

22:34
Well, we started off with a kind of silly opening, talking about data volume and emerging technologies. So what are a handful of emerging technologies, you see, that can make it difficult for people control data, especially erasing data from from managing their data, what kind of we know AI is producing our stuff? What else is out there?

22:53
One, one thing to keep an eye on, I would say keep an eye on because we, there's no need to panic at the moment. But when we think about encryption as the primary data security control encryption, of course, depends on algorithms that are sufficiently complex, that modern computing would not allow an attacker to decrypt it for hundreds of years, right, essentially making it impractical to be able to break the encryption. However, one of the concerns with emerging quantum computing is that in fact, the capability may come into place where today's encryption standards could in fact, be broken. And when we consider how much sensitive classified protected data is encrypted, that would be a game changer in terms of the risk to data. And so so a couple of things. Number one, as you can imagine, there are others thinking about this problem. This has already been at work for several years to identify post quantum computing standards. Now, interestingly enough, one of the standards had made it It started out with 69 different candidates, different algorithm candidates. And I think they're on round four or five now. But one particular algorithm had made it to round four, and very disturbingly was essentially cracked by some mathematicians in an hour using a single core PC, because they understood the math behind it, and they were able to get around it. Now, it didn't make it past round four, as you can imagine, but the fact that that and another one actually was sort of dethroned in round three, is a concern, right in the sense that we are dependent on the strength of the algorithm to protect our data. So first of all, we need to make sure that we're keeping up with that from a encryption standpoint, but also secondly, to think about other ways to protect the data. And this is where, obviously, my view is shaped by what I do on a day to day basis, but being able to reduce the data attack surface in general. meaning reduced the total amount of sensitive, classified protected data that you need to manage as an enterprise will help to make the problem more manageable.

25:10
Yeah, that sounds really good. Well, I love all the interviews I've done I've never thought of the lifecycle and I keep picking up software to them lifecycle, but John, what about data lifecycle? It's something I think has to be considered, especially with the proliferation of data from sensors and, and Jen, well, what's a generating? Well, generative is generating more data, isn't it? Yeah, it's like it's, it's almost a cycle that is this building in the building in the building. Great. Unfortunately, here, we're running out of time. You have been listening to the

federal tech podcast with John Gilroy. I'd like to thank my guest, Maurice Juanma, who is the Vice President and General Manager, Americas for Blonko technology group.

25:52
Thanks so much, John. It's been great to be with you.

25:58
Gotta turn off this recording here.