RESPONDING EFFICIENTLY TO MAJOR DATA BREACHES

U.S. GOVERNMENT AGENCIES SHOULD LOOK EXTERNALLY TO LEARN SOME VALUABLE LESSONS

By Keith Lowry

nuix

Simple. Powerful. Precise.

CONTENTS

EXECUTIVE SUMMARY

Government agencies are subject to the same explosion of data stores that every other industry continues to struggle with. More information is being created about people, and by people, every day. More emphasis is placed on Big Data, advanced analytics, data science, and whatever other name you'd like to assign to it.

This also means that your agency is very likely storing massive amounts of information about people: Agency staff, citizens, or persons of interest, it doesn't matter. And you're equally responsible to protect that information, for whatever reason you're storing it. There's no getting around that very basic reality, and part of protection involves a duty to notify affected individuals if their information has been compromised, misused, or destroyed.

Nuix can help companies meet their 72-hour breach notification responsibilities under the European Union General Data Protection Regulation. U.S. Government agencies that can meet those requirements are well placed to comply with less clearly written notification obligations.

GROWING DATA STORES AND CONFUSION

Data loss, theft, and misuse are more common in government agencies than we care to admit. Most cybersecurity practitioners concede that they can't prevent every attack they face. Coupled with the increasing value criminals place on our data, wherever it's stored—social media accounts, commercial databases, and even U.S. Government servers—personally identifiable information (PII) is one of our most valuable assets.

And this asset is growing. According to Northeastern University, "*Every day hundreds of millions of people take photos, make videos, and send texts. Across the globe businesses collect data on consumer preferences, purchases, and trends. Governments regularly collect all sorts of data from census data to incident reports in police departments. This deluge of data is growing fast. The total amount of data in the world was 4.4 zettabytes in 2013. That is set to rise steeply to 44 zettabytes by 2020.*"[i]

This explosion consists of data being collected about *us*. You may be tempted to assume that the U.S. Government should be mainly concerned with records related to government personnel, especially following the publicity and media attention that followed the Office of Personnel Management (OPM) data breach in 2015[ii]. However, from a citizen's perspective, government agencies should be concerned with the security of *all* PII under their purview, across all agencies and bodies, and their external contractors.

Because this data is *ours*, we as citizens look very carefully at those who collect it and how they go about protecting it. Government agencies have a strong obligation to identify situations where our data may be compromised and notify us in a timely manner when it is lost, stolen, or misused.

Despite this obligation, U.S. Government agencies continue to implement poor security policies and practices, especially when it comes to notifying individual victims of a breach. As you might imagine, prompt notification requires making use of a mixture of cybersecurity, incident response, and investigation tactics. It also bears closer examination into what exactly we should consider "prompt and timely" and how the government has performed so far meeting this requirement.

"As Soon as Possible"

Data breach notification requirements for the private sector vary in the United States from state to state. The U.S. Government, however, is held to a consistent, if vague, standard, as outlined in the January 2017 release titled "Preparing for and Responding to a Breach of Personally Identifiable Information,"[iii] which states:

- "Each agency shall require all individuals with access to the agency's Federal information and information systems to report a suspected or confirmed breach to the agency as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines."

- "The Attorney General, the head of an element of the Intelligence Community or the Secretary of the Department of Homeland Security may delay notifying individuals potentially affected by a breach if that notification would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions."

These guidelines don't define what "as soon as possible" means or what "without unreasonable delay" might entail. And from the victim's perspective, it's difficult to understand how disrupting a law enforcement investigation or hampering security remediation could trump my being notified that my PII has been stolen.

Going back to the OPM data breach, virtually everyone who worked in the government up to that point in time was affected. All told, approximately 21.5 million background investigation records were compromised.[iv] This means 21.5 million government employees, staff, and contractors are now *hacked for life*.[v] Even though many affected individuals assumed from the start that their own personal information was compromised, they weren't actually notified until months after the breach was made public. When they were finally notified, it often came in the form of multiple duplicated notifications over the course of several months.

Not only did it take entirely too long, in the end the government appeared disorganized and inefficient sending out its notifications. Talk about not inspiring confidence!

A SECOND EXAMPLE

When intellectual property (IP) owned by a public sector company and held by the US Government was discovered to have been stolen, the agency's general counsel's office ruled that the theft did not meet the "notification threshold." The agency never notified the IP owner that their IP (while in the digital care of the agency) was compromised. This example illuminates the fact that general counsels have a lot of leeway to interpret policies to their advantage and to the disadvantage of the data owner.

The European Union General Data Protection Regulation

By comparison, the European Union (EU) has adopted strict data breach notification guidelines as part of its General Data Protection Regulation (GDPR)[vi]. When this regulation comes into effect on May 25, 2018, it will require:

- Any organization that collects personal data from EU citizens must notify authorities of a breach within 72 hours and inform affected customers "without undue delay."
- An organization found not compliant to pay a penalty of up to four percent of its global gross revenue or 20 million, whichever is greater.

While there is still some room for interpretation with the words "without undue delay," GDPR still imposes a stringent notification requirement of 72 hours to report a breach to authorities. I'm not suggesting that the GDPR is a perfect regulation, but it is enlightening in certain areas of our U.S. Government conversation and is far ahead of anything I've seen in the United States to date.

It's also important to note here that organizations have 72 hours after they've identified a breach of their systems or information. GDPR, at its core, is not a cybersecurity regulation that is unduly concerned with perimeter defense, system monitoring, or anything typically connected with traditional cybersecurity practices. It is, first and foremost, focused on the data privacy of EU citizens. The rest derives from that singular focal point.

Detection and Response

While GDPR and other breach notification regulations or requirements aren't cybersecurity-centric by design, that doesn't mean you can ignore the pre-breach actions of detection and prevention. Building a mature detection and prevention capability is central to a reasonable, as defined legally, defense against cybersecurity threats, and should be taken seriously.

It's not a stretch to imagine that future government data privacy regulations will take a page out of the GDPR, which defines a personal breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."[vii]

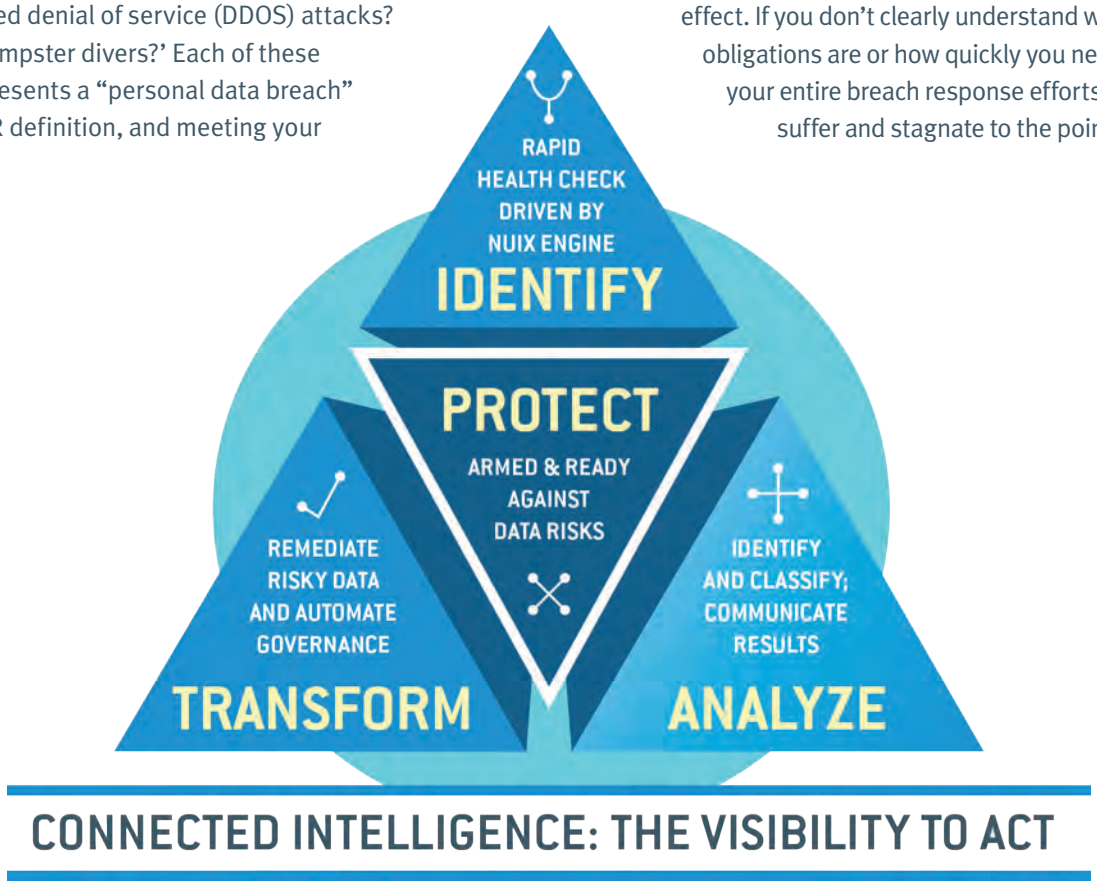
This is a broad definition, and it encompasses more than just the common perception of a data breach as "hacker broke in, hacker stole stuff, hacker is using my stuff somewhere else." What about ransomware? What about distributed denial of service (DDOS) attacks? What about 'dumpster divers?' Each of these potentially represents a "personal data breach" under the GDPR definition, and meeting your response and notification obligations in these cases will be vastly supported by a mature, dependable, and reasonable detection and protection capability.

What's My Obligation?

As of May 25, 2018, GDPR will be king of the hill when it comes to breach notification requirements and penalties for data breach notification for EU citizens.

U.S. Government agencies, on the other hand, don't have the same clear direction. They must adhere to numerous instructions and policies, including Executive Orders[viii], US Code, Office of Management and Budget (OMB) Memoranda[ix], FISMA publications[x], NIST instructions[xi], and agency policies. While the previously discussed memorandum seems on the surface to be an overarching guideline that agencies must follow, the reality is that it is distinctly murky and uncertain.

This uncertainty can have a significant downstream effect. If you don't clearly understand what your obligations are or how quickly you need to respond, your entire breach response efforts can easily suffer and stagnate to the point of inaction.



TAKING A GDPR APPROACH TO RESPONSE

Lacking any clear direction or guidance thanks to a clearly defined regulation or publication, where can you turn to make sense of a problem that you'll almost inevitably need to face?

The GDPR breach notification requirement is about as strict as you'll find. If you can satisfy its requirements, you can meet any reasonable measure or expectation for breach notification and response.

Nuix offers organizations with EU customers a platform to meet their 72-hour notification requirement. You can use this same approach to satisfy your agency's breach response requirements in a timely, proven, and reliable manner.

Safeguard Your Data

Rapid breach response begins with preparation. Act now, ahead of a breach, to better understand and prioritize the private data your agency holds. This will give you the best chance to act, and react, when you face a breach. Nuix can help you:

- Identify locations where your agency stores private data and prioritize the risk at each location
- Perform a deep content scan on all prioritized storage locations to understand what data you store that might violate data security or privacy policies
- Remediate any data that violates policy
- Establish systems and processes that protect your agency from risks of data breaches.

Once you've reviewed and remediated your data, Nuix gives you the confidence that the remaining private information is safe. You can monitor your endpoints in real-time to detect suspicious activity before it can do any real damage. While you likely already have some level of endpoint monitoring in place, Nuix's integrated platform helps you prevent breaches and gives you the intelligence and context to rapidly respond to any attacks that succeed.

Our endpoint solution allows you to:

- Automatically terminate malicious processes and prevent them from running
- Intelligently identify and block bad behaviors of known and unknown applications
- Proactively identify and catalog persons and items of interest in a centralized intelligence database to trigger an early warning the next time they show up in your network.

Rapidly Detect, Investigate, and Respond to Breaches

GDPR gives organizations 72 hours to figure out what happened and notify the appropriate regulatory bodies, once they have discovered or been informed of a breach. They also have a less specific obligation to notify affected customers "without undue delay." Nuix gives you the ability to quickly establish a complete picture of which data, customers, and systems were compromised to meet these obligations and begin breach remediation.

Using these same tools and techniques, you can use Nuix to:

- **Gain thorough visibility into activity on your agency's network and systems.** By following an attacker's tracks, you can identify which systems or areas they had control of. Nuix facilitates root-cause and timeline analysis, as well as triaging through a "rewind" or recorded data to help your team determine who did what, when, and where.
- **Quickly investigate complex incidents.** Multiple analysts and teams can work on complex investigations simultaneously to gather evidence and determine next steps, finding the answers you need faster.
- **Determine the full scope of the incident across systems and beyond.** Nuix intelligently establishes connections between seemingly disparate data in just a few clicks so your team can see how these data sets are related and who has accessed, deleted, emailed, printed, copied, or otherwise exfiltrated private data.
- **Focus on the threats that matter.** Use Nuix to pinpoint exactly who may have been affected by a breach and notify those individuals "as soon as possible."

Establish Realistic Expectations

Any kind of program to protect or understand digital activity requires technical and non-technical aspects. We've referred to this many times as taking a holistic approach to security and that hasn't changed at all.

In this case, the capabilities of your security and investigation tools combined with external regulations give you the best framework to build out policies that make sense while also letting you step forward to satisfy your data privacy obligations. I don't mean your obligation to meet some obscure and impossible-to-understand policy in a Presidential Executive Order or agency memorandum; I mean the obligation you have to protect the information your agency holds about individual people.

Write your policies with these tools and capabilities in mind. Answer the question "How fast can we reasonably expect to notify victims of a breach to our systems?" When you have that answer and have tested it using the tools at your disposal, lay it out in writing. Be honest, but also bear in mind that real people are deeply affected by your ability, or inability, to respond promptly to a data breach.

DOING THE RIGHT THING

Data breach response, cybersecurity, criminal investigations, and everything else we are "forced" to do with personal data shouldn't be just about meeting a prescribed requirement. It's easy to view these actions as a necessary evil, something to do at a bare minimum to avoid fines or punishment, to check a box on a list, or to pay lip service to in a press release or media quote.

That's not the reason at all, for any of it.

Government agencies collect data about people for a wide variety of reasons. While the subjects of that data collection might not always agree with it—you will never satisfy everyone in this regard, and we don't need to discuss the political sides of the argument here—you have a duty to protect that information from misuse, damage, and theft. Inspiring confidence in the people whose data you've collected is nearly as important as actually protecting it in the first place.

In August 2017, Congressman Anthony Brown introduced H.R. 3403, the Valuing Individual Cybersecurity Through Interagency Measures (VICTIM) Act. The new legislation proposes to create "a new role for a federal official who would serve as an interagency cyber victim coordinator," according to Adam Stone of the Fifth Domain.[xii]

Although the legislative intent appears to be reasonable, the language totally misses the digital mark. According to Stone, "If enacted, the proposed law would also require the cyber official to provide a report detailing the effects of a potential breach within 180 days, along with an annual report to Congress summarizing the office's response to attacks throughout the federal government."

One hundred and eighty days. That response window wasn't acceptable back when the Pony Express was delivering mail, let alone in the knowledge age. Your life can be totally destroyed as the result of a breach in much less than 180 days.

Until the U.S. Government gets its collective act together and makes protecting data an urgent matter, I question if it should be allowed to store and maintain any PII at all.

Consider this in closing. Which statement would make you feel better if your own data was on the line?

- "Don't worry, your data is safe with us. And if anything happens, we'll let you know about it, *as soon as possible*."
- "We'll tell you if your data was subject to a breach, just give us 180 days."
- "We've run several tests and confirmed that, if a breach happens, we can identify the problem and notify you in 3-5 days. *Our agency policy requires it; you can view the details here.*"

I know which one I'd prefer to hear.

ABOUT THE AUTHOR

Keith Lowry

Senior Vice President, Nuix USG

Keith has 30 years of experience implementing, managing, and directing insider threat, counterintelligence, and intelligence collection programs. He is a former law enforcement officer and High-Technology Crime Unit detective with the City of San Jose, California and a retired United States Navy Captain.

He also served as Chief of Staff to the Deputy Under Secretary of Defense for Human Intelligence, Counterintelligence and Security at the Pentagon, and as an information security consultant in the private sector.

REFERENCES

i Mikal Khoso, "How Much Data is Produced Every Day?", Northeastern University, May 13, 2016

ii OPM Cybersecurity Resource Center – Cybersecurity Incidents

iii Shaun Donovan, Memorandum For Heads of Executive Departments and Agencies, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017

iv OPM Cybersecurity Resource Center – Cybersecurity Incidents

v Chris Pogue, "Hacked 4 Life", Nuix, December 14, 2015

vi, vii Regulation (EU) 2016/679 of the European Parliament and of the Council, Official Journal of the European Union, April 27, 2016

viii Executive Orders, The White House

ix Memoranda, The White House Office of Management and Budget

x Federal Information Security Management Act (FISMA) Implementation Project, National Institute of Standards and Technology

xi Cybersecurity Framework, National Institute of Standards and Technology

xii Adam Stone, "Lawmakers want cyber champion for feds", Fifth Domain, August 30, 2017

About Nuix USG

Nuix USG protects, informs, and empowers the U.S. Government in the knowledge age. Leading local, state, and federal civilian, defense and intelligence agencies turn to Nuix when they need fast, accurate answers for investigation, eDiscovery, cybersecurity incident response, insider threats, litigation, regulation, privacy, risk management, and other essential challenges. Nuix makes small work of big data volumes and complex file formats. Our solutions combine advanced technology with the extensive knowledge of our global team of industry experts. We bring data to life with clarity and intelligence to solve critical data problems, reduce crime, and secure and manage information.

nuix