April 2018

SecurityAwarenessNews

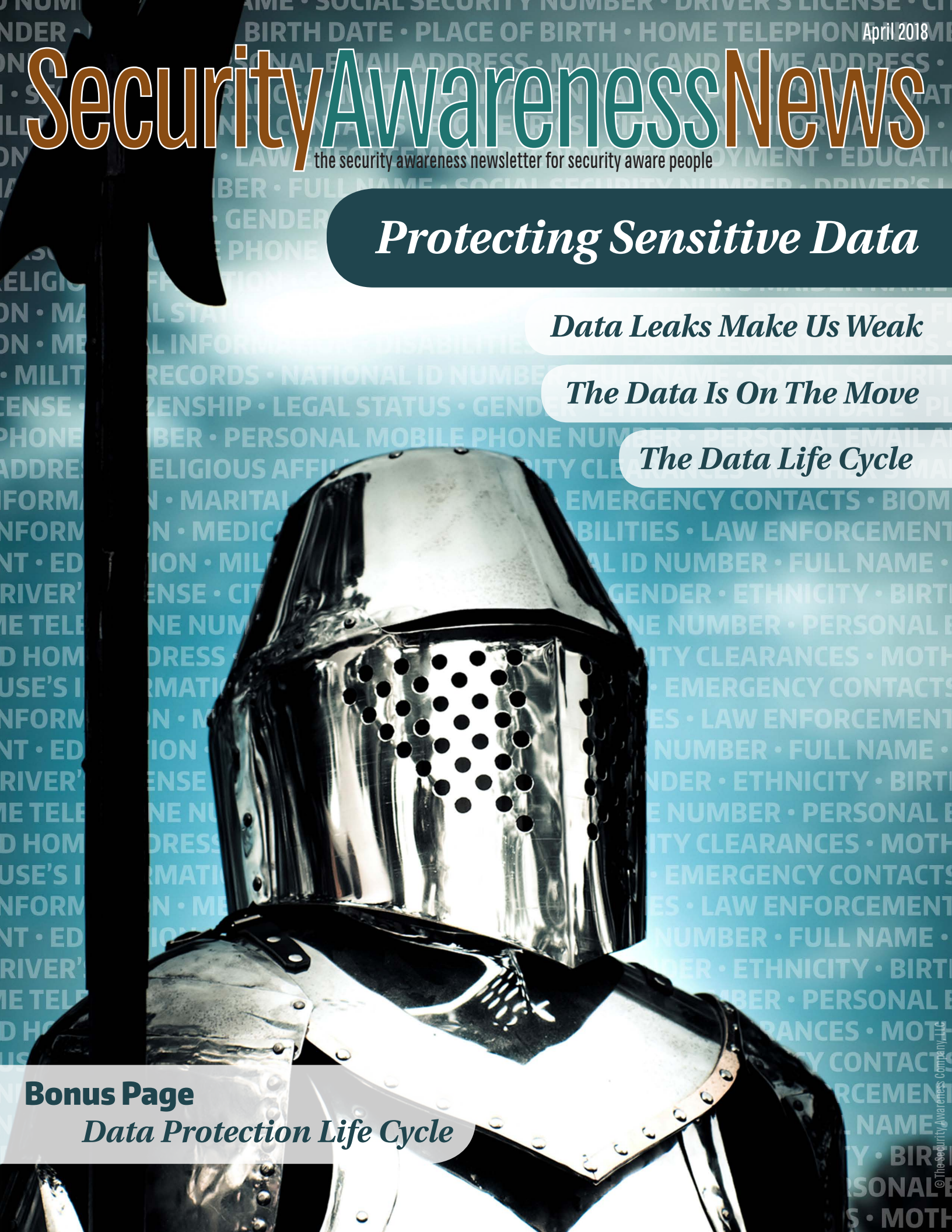
the security awareness newsletter for security aware people

Protecting Sensitive Data

Data Leaks Make Us Weak

The Data Is On The Move

The Data Life Cycle



Bonus Page

Data Protection Life Cycle

Data Leaks Make Us Weak

By now, you've heard about major data breaches like Yahoo and Equifax, both of which affected hundreds of millions of people. But another threat to our sensitive data exists, looming in everyday operations; one you may not have considered but is often more likely to occur than the mega breaches we see in the news: the accidental data leak.

Here are two real-life examples:

SCENARIO 1

An employee of a bank in Wyoming emailed, by accident, an attachment containing confidential information of over 1,300 individuals to the wrong email address.

SOURCE: http://secaware.co/2F8As0r

SCENARIO 2

The University of California San Diego sent an acceptance email to all 46,000 students who applied for enrollment that was meant only for the 18,000 that had been accepted.

SOURCE: http://secaware.co/2t7OsCu

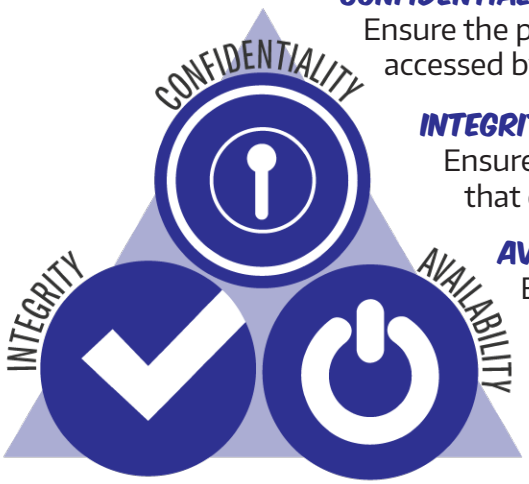
In the first scenario, personally identifiable information, or PII, ends up in the wrong inbox. Without a doubt, that fits the description of a leak or a breach. What about the second scenario? No PII was lost. No one was hacked. It was just a mistake, right? No. Careless mistakes can be costly. This scenario doesn't line up with most people's ideas of a typical data leak or breach, but the impact is detrimental to the university's reputation and to the morale of the students who received the wrong information, and could have a negative business impact as well. We must avoid these kinds of scenarios.

WHAT IF...

Instead of students receiving wrong information, a doctor received incorrect information for one of her patient's medical treatments? No one's identity gets stolen, but the results could be potentially life-threatening.

THE CIA... WE MEAN THE TRIAD OF COURSE

The accuracy of data is just as important as the privacy of data. That's why information security experts developed the CIA Triad: to provide a structured approach to help us appropriately store, transfer, and protect data.



CONFIDENTIALITY

Ensure the privacy of data such that it can't be accessed by unauthorized parties.

INTEGRITY

Ensure the accuracy of data in a manner that guarantees the data is reliable.

AVAILABILITY

Ensure the data is available and cannot be destroyed either maliciously or accidentally.

How Does This Apply To Your Job Function?

We need to consider all angles of data privacy, from the way we store data to the way we transfer data to the way we destroy data. We do this by thinking before clicking, verifying the source, ensuring accuracy, and always following policy. If you want or need more information about data protection procedures, please don't hesitate to ask!

The *data* is on the move. I repeat: the *data* is on the move.

What Qualifies as Sensitive Data?

PII

Full names, email addresses, national ID numbers, and financial information are just a few examples of personally identifiable information.

PHI

Short for protected health information, PHI is defined by 18 identifiers such as medical record numbers and health plan beneficiary numbers.

Organization Information

Any data that could cause harm to our organization or undermine our functionality, such as trade secrets and customer information, must remain private.

Classified Information

This info generally refers to government entities, though it may be declassified after a period of time and even possibly be made public.

How to Spot Sensitive Info

Before transferring any info, ask yourself these questions:

- ☐ Could it harm relationships with customers, clients or co-workers if sent to the wrong party?
- ☐ Can criminals use the info to their advantage?
- ☐ Does sharing the info break our organization's policies?

If you checked "yes" to any of these questions, then the info should be handled with the utmost care. If you're not sure, don't transfer!

3 Steps of Verification When Sending Data

1 2 3

Step 1: Verify the source. Always confirm that the person who receives the data is the intended recipient (avoiding wrong email addresses, for example) and also has authorization to access the data.

Step 2: Verify the data. Sending the wrong data to the right person is no different that sending the right data to the wrong person.

Step 3: Verify the method. Only transfer data via secure processes approved by our organization.

You can achieve all three of these steps by simply following policy! If you need clarification on our procedures or if you have any questions, please don't hesitate to ask!

Why Should You Care?

Part of living in a connected world is sharing personal information with government entities, doctors, online retailers, etc., etc. You can't obtain services without sharing your PII. But when you provide that info, you do so with the expectation that it will not be compromised in any manner. In other words, the proper transfer and storage of data is something that affects every single one of us! Apply that line of thinking to your role within our organization.

The Data Life Cycle

Data States

To better identify risks, we categorize sensitive data by three specific states:

Data in Use

Data that is actively accessed for updates, alterations, or deletions.

Data in Transit

Data that currently flows on our networks (privately) and on the internet (publicly).

Data at Rest

Data that is inactive and stored on databases and backups.

It's our responsibility to protect data at every stage of its life cycle!

Backup Solutions

A major part of information security is availability. Data is of no use if it can't be accessed. Hence the importance of backups. Our organization developed a backup strategy to protect our data. You, too, can effectively protect your data at home with the 3-2-1 backup strategy:

Three total copies, two of which are local (such as your main internal hard drive and an external drive), and one off-site (such as the cloud).

External Hard Drive • Both Windows and Mac feature built-in backup that will automatically save your data from your computer to a drive of your choosing. Alternatively, you can utilize one of the many third-party backup software options.
Pros • easy and affordable.
Cons • hard drives can fail and be destroyed.

Optical • before hard drive space was affordable, the best way to back up data was to burn it to a disc.

Pros • Long shelf life without fear of mechanical failure. Easy to store in a second location.
Cons • Limited space. Not future-proof as optical media gets phased out.

Offsite • thorough backup strategies include storing data in a second location, such as an external hard drive in a lockbox or a family member's home.

Pros • Protects your data from destruction in case of a fire or natural disaster.
Cons • Inconvenient to access or update backups regularly.

Cloud • backing up data to the cloud is a simple solution to off-site storage.

Pros • Easy to implement for multiple devices. Unlimited data options.
Cons • No control over security. Can be expensive.

WHAT IS THE CLOUD?

The cloud is hundreds of thousands of massive global data centers made up of millions of servers. More simply, the cloud is someone else's computer. When you access Facebook, Instagram, or Twitter, you are using the cloud. When you shop on Amazon or watch Netflix or YouTube, you do so via the cloud.

Is it secure? Yes and no. It's secure in a sense that your data, when using a cloud backup, is protected from destruction. Meaning, if your personal hard drive were to fail, you would still have access to your data. But once it's on the cloud, you no longer have control over security. You leave that responsibility to the cloud provider.

PROPER DISPOSAL ››› The following is intended for home use only. Always follow proper disposal policy while at work or on work devices.

Shred ››› When sensitive documents are no longer needed, shred them! How much info could someone steal by going through your trash?

Wipe ››› You can easily delete everything on your hard drive with the push of a button, but unless you use data destruction software (or physically destroy it), the data can still be retrieved. Be sure to completely wipe the drive so no one else can access it.

Restore ››› When selling or recycling a device, restore it to factory defaults, which erases all personal information.

Each stage of the Data Protection Life Cycle presents vulnerabilities that, if not for your unwavering attention and steadfast common sense, could compromise the data we are required to protect.

Preventing data breaches or leaks is a responsibility that we all share! If you're unsure of your role in this matter, please don't hesitate to ask.