PERSONALLY IDENTIFIABLE INFORMATION
DATA SECURITY

A GUIDE ON THE MANY ASPECTS OF DATA & DIGITAL SECURITY FOR THE NON-TECHNICAL READER

by the IAEE
Technologies Committee

TABLE OF CONTENTS

INTRODUCTION

The list of data-centric security standards and compliance programs is growing at an increasing rate, PCI DSS (Payment Card Industry Data Security Standard), GDPR (General Data Protection Regulation), SSAE 18 (Statement of Standards for Attestation Engagements), ISO 27K Standards (International Standards Organization), NIST SP800 (National Institute of Standards and Technology), and FISMA (Federal Information Security Management Act), just to name a few. The environment regarding cybersecurity and data security is changing so fast that it is a full-time job trying to stay on top of it.

Even without having to understand the details of data security programs, it is a struggle simply knowing what these programs mean to an exhibition organizer, how it affects the business, and understanding the risks of not paying it the appropriate amount of attention. An excellent metaphor that sheds light on the need for investing attention to data security could be holding bars of gold or cash in a safe. If the cash of a business was physically located on the premise, businesses would be very interested and active in ensuring that all manner of controls and security initiatives were implemented. There would be safe, physical controls to the safe, limitations on who knows the combination, logs of when anyone is accessing it, and logs and controls about what was happening when it was accessed.

These are all reasonable and make sense to those who may not be technology-minded. The very same types of controls must be implemented regarding digital assets. Data that an organization maintains, such as membership profiles, attendee profiles and transactions, and exhibitor information and transactions are all sensitive and valuable assets that make up a large portion of the business assets for association and independent organizers. What would it mean to an organization if all or a large portion of that data was compromised and exposed to the internet world? How much damage would result to the organization or to customers and members? It could be detrimental.

IAEE organized a subcommittee of the Technologies Committee to create this white paper to help explain the many aspects of data and digital security for the non-technical reader. The purpose is to help educate the reader on the many aspects that must be considered both within an organization and in its dealings with suppliers and vendors. Having a better understanding of the scope and breadth of these topics will enable better internal and external communications regarding the subject and help to move the exhibitions and events industry into the future with less risk.

The sections were created and organized in a way to take the reader through the various aspects of data security in a logical and building manner, although each section can stand alone and be used in the future as a refresher.

The paper begins with a discussion of the *types of data* and how to categorize the data within an organization. Then, there is a discussion regarding how to provide *governance* over the data and the training an organization may need, followed by a discussion regarding the *ownership* of PII data. Next is a brief overview of *identity access* and the management of that access followed by considerations with system *integrations*. An overview of *data in motion* and how that compares to protecting *data at rest* is followed by a deeper look at *internal security controls*. Finally, there is a brief review of considerations in an event *onsite environment*.

TYPES OF DATA AND CATEGORIZATION

Personally identifiable information (PII) is defined as "information that can be used on its own or with other information to identify, contact, or locate a single person or identify an individual in context." PII is highly valuable to an exhibition organizer and one of the key assets that make an event successful. PII is bought, sold and bartered throughout the exhibitions and events industry to prospect new exhibitors and attendees to enable growth in attendance and square footage. While this information is very helpful in retaining existing customers, and attracting new ones, this information can be exploited, which is why it is important that organizers keep it safe. If an organizer were to have this information compromised it could have adverse effects on the show's attendance, not to mention potential lawsuits from the affected individuals.

The National Institute of Standards and Technology, part of the U.S. Department of Commerce, defines the following types of data as good examples of PII:

Data Type	Data Security Standard
Full Name	High
Home Address	High
Passport Number	High
IP Address (when linked)	High
Driver's License ID	High
Credit Card Numbers	High
Digital Identity	High

Date of Birth	High
Birthplace	High
Genetic Information	n/a
Telephone number	High
Login Name	High

There is also a concept of linked PII. Some examples are:

- IP Addresses
- Cookie IDs
- Device Identifiers

For the exhibitions and events industry, it is recommended to classify data into three categories. Below are examples of the types of data. Every organization should maintain a classification of their data that aligns with the organization's security policies.

1. ***High*** – Truly confidential information that if compromised can lead to consequences for the individuals (attendees and exhibitors) affected by the breach of information. This type of information, if compromised, will have an adverse effect on the event and cause exhibitors to lose confidence in the organizer's ability to keep its personal information secure. For types of data in this category, the exhibitions industry follows the standards of the National Institute of Standards and Technology pertaining to the types of information.

2. ***Mid (PII)*** – Internal security controls are put in place to reduce the risk of accidental or intentional data loss or corruption. These are defined as other types of data, and can also be classified as PII because they can be combined or linked with other personal information to identify an individual.

Data Type	Data Security Standard
Country	Med
State	Med
Zip Code	Med
Age	Med
Gender	Med
Race	Med
Job Title	Med
Member Numbers	Med
Registration Numbers	Med
Site Login Information	Med
Business Type	Med
Number of Employees	Med
Annual Sales	Med
Exhibitor Lists with Contact Information	Med
Exhibitor IDs	Med
IP Addresses	Med
Cookie IDs	Med
Device Identifiers	Med

3. ***Low (PII)*** – All other types of data used by the exhibitions and events industry. The data cannot necessarily be used to identify an individual but should remain protected, nonetheless.

Data Type	Data Security Standard
List of Names	Low
Session Information	Low
Speaker Names	Low
Session Descriptions	Low

GOVERNANCE AND TRAINING

Information technology can deliver great benefits for an organization and can also be a source of significant risk to operations. Organizers make large investments in the people, processes and technology used to manage the information. Governance of information technology functions is essential to align the expected benefits from these critical expenditures to the goals of an organization and to manage the associated risks, including those related to the loss of the confidentiality, integrity, or availability of information.

ORGANIZATIONAL STRUCTURE

The structure of an organization is an aspect of governance that may not come immediately to mind when considering information security, but it is important. Accountability and clearly defined roles (which need not be fixed, inflexible, or immutable) are important for every part of an organization including an information technology function.

"Accountability and clearly defined roles…
need not be fixed, inflexible, or immutable…"

A very common approach to granting individuals permission to perform certain actions is securing software features based on the requirements of the job of that person, an approach known as role-based security. Obviously, if roles have not clearly been defined, assignment of security based on those roles is going to be difficult or impossible. This in turn will lead to access being assigned to individuals on a case-by-case basis, which is a cumbersome approach that can be difficult to manage in large organizations, or worse, people will be given permission to do everything with no consideration to what their job actually requires.

Another consideration related to organizational structure is how the interaction of jobs or roles affects the security of the data. Most individuals have seen checks that require two signatures or are familiar with an additional level of approval being required if an expense exceeds a certain threshold, a concept called dual control. Knowing that information is valuable, how many people would it take in an organization to substantially reduce or maybe even destroy its value? Could those individuals write checks for a similar amount without any approval?

CHANGE CONTROL PROCESS AND LEADERSHIP

Trust is not the only factor in determining whether or not to put such controls in place. While there is no shortage of malicious actors in the world, an organization's information is exposed to risks from accidents as well. Having a change control process in place that requires another person to validate a change, for example, might help to prevent someone from accidentally making a change to a system that would be an innocent yet costly and disruptive error.

Costs associated with controls to mitigate these kinds of risks will exceed the benefits to the organization of mitigating them. Investments of time and energy into securing data will need to be balanced with the priorities of the organization as a whole. Making these kinds of decisions is what governance of enterprise information technology is all about. The consequences of failing to make such decisions appropriately can have severe consequences for an organization, including rendering it incapable of continuing operations. The organizational structure of and assignment of responsibilities to senior management (e.g., whether or not to have a Chief Information Security Officer to address some of these questions) will determine how effectively these decisions are managed and ultimately how secure an organization's data is.

Those who govern an organization also create the environment within which all security controls operate. If an organization's leadership is corrupt or unethical, security is bound to be compromised. An important part of governance is communicating the organization's standards for ethics and competency. Such communication can be formal or informal, but organizational policies are the primary formal tool for such communication.

"An important part of governance is communicating the organization's standards for ethics and competency."

INFORMATION SECURITY POLICY/INCIDENT RESPONSE PLAN

An information security policy is needed to describe classifications of data, such as PII, and the expected standards for handling that data. The policy might also address:

- Defined roles and their responsibilities
- Change control processes
- System configurations
- Backup and recovery procedures
- Software development standards
- Employee training requirements

An incident response plan and an acceptable use policy may be included in the information security policy or they may exist as separate policies.

The organization should prepare an incident response plan to enable it to respond effectively in the event of a data security breach. The scope of the plan should be clearly stated, including:

- How incidents can be identified and how they should be classified.
- Different responses based on the classification of the incident, taking into account all legal and contractual notification requirements.
  - The steps that might be necessary to contain the damage from whatever has caused the incident including removing any compromised systems and recovery of any data or systems damaged or destroyed as a result of the incident.
- Last but not least, the plan should provide for a time to review the incident, perform a root cause analysis, and note any lessons learned.

The incident response plan should be tested at least annually to evaluate its readiness in the event of an actual breach. Legal considerations must be taken into account based on the location of the affected individuals and the nature of the breach.

KEEPING EMPLOYEES INFORMED

An acceptable use policy can be used to inform employees and other users of the systems what activities and uses are permitted on systems and what uses are prohibited. Employees should be informed that their use of the systems are subject to monitoring, and their expectation of privacy should be limited. Reinforce with employees the expected standards of conduct for e-mail and internet, and the expectation that the confidentiality of the organization's information will be maintained at all times. Acceptable uses of employee-owned devices and software on the network and systems should be considered as well.

Training is another important way management communicates organizational standards. Security awareness training for employees is an important step to help secure data. Most people are trusting and do not think like criminals, which is something that scammers will try to use to compromise an organization's systems. ***Tailgating***, the practice of following closely behind an employee who has opened a secured door, is a common example of abusing the good nature of people. Training should be conducted at least annually.

"Most people are trusting and do not think like criminals,
which is something that scammers will try to use to compromise your systems."

PHISHING

The security awareness program must include training on phishing. Phishing is the practice of sending emails to users to induce them to divulge confidential information or to install malicious software on their systems. Phishing that is directed at a highly specific target, perhaps using detailed information already known about the target, is known as spear-phishing. Users at all levels within an organization must be vigilant in their efforts to avoid opening attachments and clicking on links in emails. Ransomware, malicious software that steals or destroys information and then attempts to extort a payment to recover it or prevent its release, is frequently introduced through phishing campaigns.

Users should be told to be skeptical of any email they receive that they were not already expecting, particularly if it attempts to convince them that urgent action is required on their part. They should be educated to always hover over links to web pages to find out where a link will go and pause before clicking

anything. If an email claims to be a communication from a well-known company asking someone to log in, users should open their web browsers and type in the address of the company's main web site instead of following the link in the email.

Tips to provide users on recognizing potential phishing emails are:

- first impression is that there is something odd about the email
- sender is unknown or is someone with whom the individual does not usually communicate
- email was not specifically sent to an employee
- email was sent from an odd location or at an odd time
- subject is not specific or is unrelated to the body of the email
- email is asking an individual to open an attachment
- email attachment is recognized as a "dangerous" type
- body of the email uses poor grammar or contains language that is awkward or inappropriate.

DATA OWNERSHIP

Once data has been categorized, the next necessary step is to identify the information assets that an organization owns, controls, or processes. Typically, the only data an organization confidently owns is the data that is independently created. Generally speaking, PII is created and owned by individuals and controlled or processed by organizations. When and how individuals create PII, and whether or not individuals can ever assign the ownership of their PII to another entity, and if so how much, is lately a matter of considerable ethical and legal debate. A helpful way to think about collecting and safely using PII might be to think of it as borrowing the PII from the individual without ever really "owning" it.

RESPONSIBILITIES OF DATA OWNERS

The European Union General Data Protection Regulation (GDPR), to be enforced beginning in May 2018, regulates the processing of PII, which the GDPR calls "personal data," of EU residents. The GDPR has maintained the distinction between data controllers and data processors found in the 1995 Directive. Data controllers collect PII and have many responsibilities with respect to the data collected. As agents of the data, both data controllers and data processors have a responsibility to process PII, in accordance with the policies and instructions that have been developed, as well as comply with applicable laws and regulations. The most important idea to take away from this distinction is that those who collect PII have the most responsibility for the proper handling of that PII. Some of those responsibilities are:

1. ***Awareness***

   If borrowing an asset, the first consideration is to make sure the asset's owner is aware. If an organization is in the habit of "borrowing" things from people without letting them know, sooner or later the organization will have legal trouble. The collection of PII works much the same way. For example, if cookies are being used to collect information about visitors to the event web site, those visitors should be made aware and consent obtained from the visitor prior to the collection of their PII.

2. ***Choice and Consent***

   After individuals are made aware that PII is being collected, the next step is to obtain their consent for the purpose the data is being collected and give them the choice whether or not to accept that collection. Documenting consent is important. To be sufficient, consent must be freely given, specific, informed, and unambiguous. Clearly describing the way in which the PII is being collected, and what for what purposes it will be used, so that the individuals involved can give their informed consent is also important. Before PII is collected, the organization needs to have a good understanding of what specific information needs to be collected and why, and for how long the data will be kept. Once this is known, explain it to individuals whose PII is being collected, and obtain their consent.

   Generally speaking, consent should be explicit whenever EU personal data is collected, transferred, or otherwise processed. Opt out or implied consent cannot be safely relied upon, and so PII should only be collected with the specific opt in consent of the individual.

3. *Use and Maintenance*

The PII should only be used for the purposes for which the organization previously obtained consent from the individuals involved. Individuals may change their minds about letting their PII be used and that an organization is responsible for giving them a way to revoke their consent and have their PII deleted.

If individuals do consent to use of their PII, an organization has the responsibility for maintaining the integrity of the PII as it is being used. Employees should be trained on the proper handling of PII. Systems should be designed and tested so that PII does not become corrupted. Securing systems that handle PII is necessary to prevent its unauthorized use or alteration.

The individuals from whom PII is collected should also have the ability to correct their own PII. Among other things, this means organizations must have a process in place that enables individuals to obtain whatever PII of theirs is stored on systems so they can identify any errors that need to be corrected. Organizations also need to have a way for those individuals to submit changes to their PII so they can correct it. There may be a dispute at some point over what information is correct; organizations will need to plan for a way for individuals to escalate their complaints and possibly invoke an independent arbiter to resolve the dispute.

4. *Retention and Disposal*

Going back to the analogy of borrowing an asset, borrowing an asset for an indefinitely long period of time begins at some point to correspond more to a description of taking rather than borrowing. PII should be retained only as long as necessary to satisfy the purpose for which it was collected, and should be disposed of once the PII is no longer necessary to fulfill the purposes for which it was collected. Indefinite retention of PII can be a liability. Organizations should have retention policies for all PII collected. Contractual requirements, regulatory requirements and legal requirements are all important considerations when drafting a retention policy for PII.

PII that is no longer needed should be disposed of securely. In most cases, simply deleting information is not sufficient to preclude recovering the information by using specialized recovery tools. When disposing of PII, special utilities may be needed in order to wipe the data storage device clean. When flash memory devices are used, like USB thumb drives or solid-state drives, there is no guarantee that the memory will be overwritten if a file is overwritten.

Also, keep in mind that some hard drives or other devices might fail in such a way that recovery using a normal computer is impossible but that the device components might be transferred by a malicious actor to working hardware and read that way. Having a plan for physical destruction of data storage devices is a good thing to have in place in advance of needing it. Part of that plan might be establishing a relationship with a vendor that can securely destroy physical devices and that offers a certificate of destruction once that destruction is complete.

5. *Vendor Management*

Once policies and procedures have been put in place to protect PII, vendors must be held to the same standards. The GDPR places direct regulatory obligations on both data controllers and data processors to protect and control PII. Apart from potentially being a legal requirement in some jurisdictions, coming to a good understanding of who is responsible for what and writing that down into performance clauses in a contract is just a best practice. It might be helpful to use a table that is shared with the vendor to indicate for each responsibility who is responsible for what elements.

Sometimes monitoring the status and qualifications of vendors can be streamlined by using a public source (e.g., company website, LinkedIn) that is available to confirm vendor qualifications. Reports from independent third parties as well as specialized audits can also be used.

"The most important idea to take away is that those who collect PII have the most responsibility for the proper handling of that PII."

IDENTITY ACCESS AND MANAGEMENT

Identity and access management (IAM) is a term that is used very broadly and encompasses many subjects. IAM refers to the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources." Terms that are erroneously used as synonyms include multi-factor authentication, single sign-on, role-based authentication, etc.

A critical key to success in securing PII is a strong ***digital identity*** and access management strategy. Sound IAM planning will give an organization confidence in the approach and visibility into the efficacy of the policies. Further, it will allow the organization to establish trust with the people accessing and administering information on its event sites, management portals, etc.

DIGITAL IDENTITY

In the everyday world, individuals hand over physical identifiers to share information necessary to conduct their lives. A license, passport, club membership or employee badge are all physical forms of identity that may contain information that is unique to a person. Similarly, a digital identity allows its holder to be identified uniquely within the context of a system or across multiple systems. A digital identity consists of the following:

- ***Identifier*** – This is a core piece of information in a digital identity. It is unique among all other identifiers in the same context and ties together the other components of a digital identity. Examples include an email address, numeric code or a globally unique identifier (GUID).
- ***Credentials*** – This is the information that is used to validate the authenticity of a claim to an identity. It can be a username and password or a public/private certificate combination. In each case there is some secret information known only to the person trying to authenticate and to the system of record.
- ***Attributes*** – This is auxiliary information that describes the individual being identified or describing the individual's relationship the system. Examples include name, address, preferences, etc. Often this information itself is PII.

POLICIES, PROCESSES AND TECHNOLOGIES

As the definition indicates, IAM is comprised of three primary elements: policies, processes and technologies. Policies are the constraints and standards that are necessary to comply with regulations and business best practices. Processes describe the workflow that leads to the completion of business tasks or functions. Technologies brings the identities, policies and constraints together to accomplish business goals in a more automated and accurate way.

KEY TECHNOLOGIES

As mentioned earlier, IAM is a very broad topic with many areas of concern. Three main areas of technology that make up an IAM system:

- ***Directory Services*** – Digital identities (identifier, credentials, attributes) need to be stored securely and organized. Similarly, security policies and identity access entitlements need to be securely managed and discoverable. Directory services is like a secure database that houses this information.
- ***Access Management*** – This refers to the process of controlling and granting access in response to resource requests. Processing a request involves authentication, authorization and auditing. Authentication is to ensure the validity of a 'login' attempt. Authorization determines what actions an identity is allowed to perform or what data it is allowed to access.
- ***Identity Lifecycle Management*** – There are actions that need to be taken in each step of a digital identities lifecycle. From creation to utilization to termination, each portion has a multitude of scenarios to consider. Think hiring an employee (creation), changing a password, promoting an employee (increased privileges) and terminating an employee.

Organizations are made up of people and systems. People are represented within the IT systems as digital identities. Everything that occurs in businesses is the consequence of actions initiated by and for those identities. Regardless of the size of the organization, there are numerous ways to tackle the complexities involved with managing these identities throughout their lifecycle. While the importance of individual requirements may vary by industry, each of the areas of concern mentioned here are real for any enterprise.

WHY THE ORGANIZATION SHOULD CARE ABOUT IAM

A solid IAM strategy directly affects the security and productivity of a company, but sometimes its lower visibility can make it difficult to obtain sponsorship and funding. IAM is most commonly employed to help secure PII, digital assets and infrastructure, but of equal importance, it can help enhance business productivity and increase competitive advantage. Some benefits include:

- Opening doors to customers, partners, suppliers, contractors to increase productivity, efficiency of partnership and satisfaction
- Getting control over the plethora of mobile devices, laptops, tablets and bring your own device (BYOD) endpoints
- Reduce support interactions to the important ones (e.g., allowing automated password resets)
- Reduced risk to internal and external attacks
- Greater centralization of your compliance efforts

"IAM is most commonly employed to help secure your PII, digital assets and infrastructure, but of equal importance, it can help enhance business productivity and increase competitive advantage."

However, when an IAM strategy is ignored or done poorly, the organization may suffer from:

- Lost User Productivity – Users lose time as they wait for new accounts to be created or new resource access.
- Poor User Experience – Having multiple user accounts and passwords in order to gain access to different applications and resources is cumbersome.
- Limited Information Sharing Across Applications – Applications are "siloed" by being unable to share basic information such as contact details.
- Unnecessary Administrative Overhead – Help desk and other IT support staff are unnecessarily burdened by support requests for basic account management.
- Reduced Security Stature – The inability to streamline deprovisioning of users or to manage user access privileges to applications and resources exposes your organization to the risk of unauthorized access and audit compliance issues.

REVIEW OF IAM STRATEGY

If an organization is unsure of the robustness and completeness of its current IAM strategy, it is time for a review and audit. If in-house expertise to complete this review does not exist, there are specialty security companies that can help. The IAM strategy does not remain static over time. As new technologies emerge, business models change and constraints evolve, to the IAM strategy plan will need to be continually adjusted. Keeping up with the latest threats, security guidelines and industry specific concerns can seem daunting when attempted all at once. If an organization does not have an IAM solution in place already, it should assign a team to take on this effort in small chunks, continually. Like many other efforts in securing PII, IAM is a journey, not a destination.

INTEGRATIONS

Integrations in the exhibitions and events industry are typically a connection of two or more systems that allow data to flow between them automatically. Integrations are used to create internal efficiencies, ensure accuracy across systems and create a better user experience for exhibitors and attendees. PII is usually part of this data flow; organizers will want to know all the data being shared and ensure it is secure.

TRUSTED VENDOR PARTNERS

Before setting up any integrations, be sure to work with trusted vendor partners that can provide secure data transfer. Begin by requesting they share their data transfer security protocols and discussing some of the other topics in this paper. Ideally, the IT team will be included in these discussions and will review their security documentation. Any discussions and requests made can build more trust in the vendor(s) the organizer is working with on integrations. Whenever possible, try to ask for data security and integration processes in the RFP and include it in any agreement(s) signed.

If an integration between two or more vendors will occur, be sure to bring them together to discuss PII security. Their technical leads who can speak to the details of how they will transfer data securely should be included in the meeting. Doing so will add as an additional check because one vendor may have higher standards in regards to data security they can share with the other. The vendors' IT staff and expertise should be an extension of the event team.

DATA MAPPING

Data mapping is an important step in understanding exactly what data is being transferred via integrations. A system map can give a general idea of how data flows, but a more detailed data map that lays out each piece of data shared from the system and/or between vendor systems should be created. This data map can serve many purposes and it will help determine everywhere PII is being shared and stored.

Data maps can also provide a visual where PII is created or can be edited. Understanding this will help know where to implement further controls as well as identifying opportunities to gather and use that PII for other initiatives.

This data map can be as simple as an Excel file, where each row is a different piece of data and the columns show different attributes:

- Label in each unique system

- Sample Value
- Where it Originates
- Is it editable or locked in certain systems
- PII or Public
- Other notes on how to treat that field

AMS Data Field	Vendor A Data Field	Vendor B Data Field	Sample Value	Where it Originates	PII or Public
Vendor ID	Exhibitor ID	Username	111222333	AMS	PII
Company Name	Company Name	Exhibitor Name	Google	AMS	Public
Exhibiting As Name	Exhibitor Name	Booth Name	Google Inc.	AMS	Public
PC First Name	Primary Contact First Name	First Name	James	AMS	PII

ACCESS CONTROL

Once setup integrations have been created, assess who has access to what data in each of the unique systems. The data map will help to understand what sensitive information is stored in each system so decisions can be made on the appropriate people to have access to that data. The organization will likely need to work with trusted vendor partners to setup this access and establish how best to eliminate unnecessary access.

DATA IN MOTION

Data in motion is data actively transferring from one location to another. During that transfer, data is at its most vulnerable. Not only is data in transit potentially more accessible to cyber criminals it is also at risk of human error in transmitting to the wrong locations.

WHERE TO START

- Define who needs what data throughout the show cycle and how that data will be moved from one location to the other.
- Understand all the parties who have access to the data while it is in transit.
- Identify the specific fields that are the most in need of protection (i.e. passwords). If the decision is made that those specific fields are required to be shared, then a strong encryption method must be used. See below for a brief overview of the various currently available.
- Implement robust network security controls to help protect data in transit or ensure that vendors have the expected security controls. Network security solutions, like firewalls and network access control, will help secure the networks used to transmit data against malware attacks or intrusions.

ENCRYPTION

Encryption is the use of various methods to turn plain text into an unreadable code. For this discussion encryption is recommended in two different ways:

- Encrypt the transmission over a secure channel – The list below gives some examples of secured channels for data transmission

	Instead of...	Use...
Web Access	HTTP	HTTPS
File transfer	FTP, RCP	FTPS, SFTP, SCP, WebDAV over HTTPS
Remote Shell	telnet	SSH2 terminal
Remote desktop	VNC	radmin, RDP

- Encryption of specific pieces of data (i.e. passwords) – There are three basic encryption methods widely used today:

    1. ***Hashing*** – creates a unique, fixed-length signature. Hashes are created with an algorithm or hash function. A one-way hash cannot be reversed or deciphered

2. ***Symmetric*** – use of the same key by both the encrypter and the decrypter. There are many forms of symmetric encryption with the key size and strength being the biggest differences. The challenge is to securely store and use the shared key.

3. ***Asymmetric*** – two keys are used. The encrypter uses a public key and the decrypter uses a unique private key.

EMAIL

Traditionally, in the exhibitions and events industry, a lot of data has been transmitted amongst staff and their vendors through email. While convenient, without the right security and policies in place this is another potential avenue for data loss.

- Develop a policy of what information employees can send in email
- Use compliance software to check all outbound and inbound emails for sensitive information such as credit card data
- Data sets should not be sent in email unless fully encrypted
- Enforce a policy that prohibits data sets being sent to personal email accounts not under the security measures established by your organization
- Regularly review email security risks, and how to avoid the risks, with all employees
- Implement security best practices for allowing employees to use personal devices to access corporate email
- Ensure webmail applications use secure logins and encryption
- Use spam filters and anti-virus software
- Avoid accessing company email from public Wi-Fi connections.

DATA AT REST

"An ounce of prevention is worth a pound of cure."
– Benjamin Franklin

OVERVIEW

Data at rest refers to inactive data that is stored physically in a digital form or, less commonly, in paper form. Data at rest is most synonymous with backups or archives. An organization can hold a treasure trove of valuable data. Show managers likely have contact information for all exhibitors, attendees, and facility personnel. Securing this data is a big responsibility and must be taken very seriously. There are several methods to ensure that sensitive data is kept in the right hands. This section includes an overview of how to secure data through encryption, file and folder permissions, data isolation, and proper storage of physical assets.

ENCRYPTION

Using encryption offers a dramatic increase in the safety of data. When implemented correctly, the likelihood of someone getting access to usable data is reduced to nil. Breaking strong encryption requires an incredible amount of effort and computer resources.

Encryption comes in many forms but almost all are secured through a password. As with computer systems, maintaining a strong password is essential. It is imperative that only the necessary people have the password.

There are many backup software programs that support encryption, such as CrashPlan, to simply encrypt the entire storage drive. Many modern operating systems have this capability built-in.

It is important to remember to close out of the encrypted files, folders, or drives once done accessing the files needed. This will prevent someone else from walking up or connecting to the computer and accessing the encrypted files. Think of the encryption as a safe. No one would walk away from an open safe that is full of money.

PERMISSIONS

When data is kept on servers, it is imperative to have the users' permissions set correctly. It is even more critical if there is sensitive data at rest on the same server. The system administrator must get very granular with which users have access to which folders. For instance, not everyone should have access to human resources, accounting, or other sensitive folders. The same type of thinking must be applied to data as well. Restrict permissions to only those users who actually need access to those folders.

An occasional audit of users and their permissions will shed light on any unwarranted access the user might have. When an employee leaves the company for whatever reason, all access that they had must be disabled – VPN access, workstation access, email access, etc.

DATA ISOLATION

The more data is isolated from networks and people, the more secure it becomes. There is a balancing act that needs to be done in regards to ease of access for authorized users. Although it is straightforward that the more sensitive the data, the tougher it needs to be to gain access.

- ***Network Isolation*** – Keep important data off of the main network. Work with IT to figure out the best course of action.
- ***Computer Isolation*** – If the data is stored on a single PC or a server, limit physical access to that computer. This also could fall into network isolation if the computer is connected to a network, it likely is.

PHYSICAL INFORMATION/DOCUMENTS

Physical document management is an important aspect with respect to data. People may print off emails, invoices, credit card information, personal records, etc. This can mean filing physical documents away in a locked cabinet or, if they are no longer needed, shredding them with a cross-cut shredder in accordance with the organization's retention policy.

Each organization is different, with different data on hand and different levels of data protection requirements. Involving human resources, information technology and any other applicable department in any discussions involving customer data will make everything much easier in the end.

INTERNAL SECURITY CONTROLS

Information is one of an organization's most valuable assets and it needs to be treated that way. If all of the time, energy, and investments made in developing the information an organization possesses were turned into something tangible, like a giant pile of cash or an expensive work of art, what sort of rules and safeguards would naturally be put in place to protect it? Many data security measures are analogous to controls that people are encountering in their lives, but they may seem unfamiliar in some cases because information sometimes exists in an intangible form, like electronic bits stored somewhere in "the cloud."

> *"If all of the time, energy, and investments made in developing the information you possess were turned into something tangible, like a giant pile of cash or an expensive work of art, what sort of rules and safeguards would you naturally put in place to protect it?"*

PREVENTATIVE CONTROLS

Internal security controls are put in place to help reduce the risk data will be devalued from corruption or loss that can be either accidental or intentional. Ideally, such controls would help to prevent the possibility of any loss before it occurs. If preventative controls fail, then controls designed to detect that data is in the process of being corrupted or lost would help to stop that process while it is happening. If data corruption or loss has occurred, corrective controls can help restore its value if that is possible or at least reduce associated additional losses if it is not.

Part of managing the risks is to think about the consequences of an internal breach, working backwards to ask questions about what might have prevented the negative outcomes or would have at least reduced the negative effects.

USER PERMISSIONS

One of the first questions might be who had access to the systems by checking the log of which users are signing into systems and when. Users requests for data should be logged and the purpose documented. Controlling access to data this way can help to know if any of the data has been accessed or used in an illegitimate way.

Limit the number of people who have access to the systems and be sure that only the people who need access are authorized access to just the areas necessary, based on their documented job duties or role. This approach is used to protect data and is called the principle of least privilege; people are given access to only what data they need to perform their assigned duties or roles.

"Log user requests for data and document what is being done with it."

KEEPING UP WITH AUTHORIZATIONS

When a person is hired, or changes roles, is when access should be given to the person. When the employee leaves, their permissions are removed. Documented processes should be in place to cover all scenarios.

Not removing access when a person changes jobs within a company is a frequently-observed problem that results in what is known as privilege creep. Longtime employees who have worked in many capacities might wind up with all kinds of access that they do not require in their current role. Another consideration is when previous employees are rehired. If access to individual software applications is not removed as part of the termination process, for example, then if a former employee is rehired, perhaps to work in a new, part-time capacity, that person may have more access than needed to perform the duties of the new job.

Rarely are procedures correctly executed all of the time. Periodic reviews of access, perhaps quarterly, are a necessary corrective control. Extending the safe analogy further, an authorized employee, who normally accesses the system at 8:00 a.m., suddenly accesses the systems at 11:00 p.m. might call for additional investigation of that activity. Establishing a baseline of normal user activity, such as how and when access privileges are being used, and then periodically reviewing user activity against that baseline is a good control to have in place.

THIRD PARTY CONTROLS

Third party contractors and vendors are under close scrutiny by auditors. When establishing new relationships, due diligence should be exercised and any contractors or vendors who have access to an organization's data, or with whom they share this data, should be thoroughly vetted. If applicable, consider asking the contractors or vendors for independent confirmation of their security practices. Just like employee access should periodically be reviewed, vendor access to data and its compliance with required security controls should be reviewed, at least on an annual basis or when a contract is being renewed.

"Just like employee access should periodically be reviewed, vendor access to data and its compliance with required security controls should be reviewed, perhaps at least on an annual basis or when a contract is being renewed."

One technique is to monitor the use and protection of data by third parties is to seed any data extracts provided to them with information that would enable you to recognize the source of information that had been improperly disclosed. For example, when providing a mailing list to a third-party marketing company, add in a few records with contact information that would result in a person within the organization receiving any mail that was improperly sent to the list.

TRAINING

Employees must be trained on the secure handling of confidential information such as PII or other sensitive data, like financial account numbers. Do not neglect the training of contractor or vendor employees. Make sure that all persons who handle information have been sufficiently trained. When providing contractors or vendors access through an organization's systems or facilities, policies should be in place to closely monitor their activity. The goal should be securing the information regardless of who is processing it or where that processing is done.

SOFTWARE AND FIREWALLS

Many of the controls mentioned so far have focused on employee activity. However, those controls would be insufficient by themselves. The systems that process and store data need to be protected against attacks as well. The organization should strive to maintain a layered approach to security, known as ***defense in depth***, so that if any one control fails, it will not result in a compromise of the system.

- Firewalls
- Antivirus Software
- Testing Software
- Mobile Devices

Firewalls in a computer network are like a fence around a store, making sure that access is going in and out only in the places and ways that it is supposed to. If the firewall fails, having an intrusion detection system, or an intrusion prevention system, dishonest individuals who breached the breached the firewall from being able to gain access undetected. If the dishonest person makes it past the firewall, one more layer of defense would be antivirus software installed on the computer systems to prevent the installation of any malicious software, or detect it and correct the configuration of the systems by removing or quarantining it. And if all else fails, employees trained in security awareness might recognize the abnormal behavior and report the threat.

"The organization should strive to maintain a layered approach to security, known as defense in depth, so that if any one control fails, it will not result in a compromise of the system."

Another important aspect of maintaining internal security controls is to make sure all of the software and devices used are up to date on their latest available security patches. Antivirus software must be updated with the latest available signature definitions. Vulnerabilities are usually immediately exploited once they are publicly announced, so updates should be applied frequently or if possible, automatically when they are published. Antivirus signature definitions should be updated at least once a day and preferably more frequently than that.

The only way to be assured of the effectiveness of security controls is to test them. Because vulnerabilities are published on a daily basis, consider the routine use of software to scan for those vulnerabilities. Any vulnerabilities identified should be evaluated for the risk they present and prioritized so that the vulnerabilities representing the greatest level of risk are addressed first.

Mobile devices, like laptops and cell phones, may require additional security controls because they will most likely be used outside of the secured internal systems. All devices should be password protected and use some sort of whole-disk encryption scheme so that if the mobile device is ever lost, the information on the device is not recoverable. The ability to remotely wipe the contents of a device clean can also be useful, however that ability usually requires connectivity to a network and malicious persons may block such access before the commands to wipe the devices can be sent to the device. Host-based firewalls, if available, should be used to provide an additional layer of protection.

ONSITE CONSIDERATIONS

When an event is occurring, most of the security considerations that existed pre-event are still relevant and can be even more important than when operations are in-house. In addition to those considerations, an on-site environment presents additional challenges to security.

Managing vendors on site is complex, but managing the relationships with these vendors is essential for the protection of PII.

"Written agreements with vendors should set clear expectations for service delivery levels with regard to the handling of PII and explain who is responsible for each control that will be put in place to secure data on site."

Do not assume that operations managed by vendors are secure or that protections will be in place onsite. Risks can be transferred but accountability cannot. Ultimately, the organizer is going to be held accountable by members, attendees and exhibitors for the security of their PII. Appropriate steps should be taken to ensure vendors are following the same security practices onsite as the organization would follow to keep the PII secure in the organization's own systems, and document those requirements in written agreements with the vendor.

"Encryption should always be used when transferring PII data through the networks of on-site service providers."

Some facilities may offer the option of a private network or VLAN. However, changes to these networks are being made frequently and configuration errors do occur. Detecting such misconfigured networks can be tricky to impossible even if there is no malicious intent. While a private network on site might be beneficial in terms of network stability or performance, it is insufficient as a security control.

"Encryption of data at rest should also be employed when PII is stored onsite."

Theft of computers or laptops onsite is always a possibility, as it is when data is stored in house, but in addition to that risk, these or other devices may be staged in areas that are not completely secure while they are waiting to be deployed or they can simply be lost in transit somewhere along the way. Encrypting data at rest helps to mitigate the risks associated with such losses.

"All wireless communications should be encrypted and be transmitted using the WPA2 protocol."

Wi-Fi Protected Access II (WPA2) is the most secure wireless protocol that is in common use. Wi-Fi Protected Access (WPA) is older and not as secure and WEP is not secure. However, as with the private networks discussed previously, no assumption of privacy on these networks should be assumed and PII transmitted across these networks should also be encrypted.

When wireless networks are used, users must be vigilant and heed any security warnings that are reported because wireless networks can be compromised without the need for physical access that is required to compromise wired networks. Rogue wireless devices and networks will also likely be present in and around any on-site environment.

Special attention needs to be paid to systems that are to be integrated in an on-site environment for several reasons:

- Ensure they do not communicate in plain text
- Ensure they do not require specific ports to be opened that cause vulnerabilities
- Ensure private, segmented network connections that are limited to approved parties are being used.

In regards to network segmentation, while many networks will be carved into different segments intended to isolate systems for performance and security reasons, once again this cannot be assumed to be the case in an on-site environment. Unlike an in-house network, devices may be sharing a network with all manner of unknown and untrusted devices.

"Use a firewall between any untrusted device or network and any trusted device or network."

In an on-site environment, a trusted computer should be secured by utilizing a host-based firewall, which is sometimes also called personal firewall.

"Physical security is perhaps the biggest difference between operations in house and those on site."

The following best practices should be followed:

- All devices need to be secured and inspected for any signs of tampering, especially if they are left unattended for any period of time
- Employees and temporary staff authorized to work in areas where systems are present must be clearly and easily distinguished from visitors or others who are not authorized to be in those areas at all
- A clear desk policy should be enforced at all times when working with hard copy forms or reports that contain PII so these hard copies are not removed, copied, or viewed by unauthorized persons
- Computers should be hardened against compromise and installation of malicious software like key loggers; locked when not in use; and have screen savers installed that should lock computers automatically if they have not been in use for a certain amount of time, typically fifteen minutes or less

Finally, consider system redundancy, operations resilience, and the ability to recover from system outages on site. If systems depend on internet connectivity provided by a venue, determine whether uptime statistics represent an acceptable level of risk or an alternate means of connecting to the Internet is required. Make sure that information is being backed up securely and can be recovered securely. When redundant systems are put in place, make sure they are configured the same as existing systems so security is not reduced if these systems have to be put in place.

CONCLUSION

The hope of this IAEE Technologies Subcommittee is that this document will help explain and expose event organizers that may not have technology backgrounds to the breadth and scope of the very current and important topic of information and data security. At the very least, the intention is to educate and provide an impetus for extended conversations within organizations and beyond into the vendor environment as to how these collective teams will meet the growing challenges and risks regarding the protection of one of the most valuable assets – data.

A special thanks to IAEE in support of this important topic, to Jodi Yauch and Scott Stanton, CEM, CAE from IAEE for their participation and support, as well as to all the contributors from within the IAEE membership for their time and participation. Without these volunteered efforts this project would not have been possible.

2017 IAEE TECHNOLOGIES SUBCOMMITTEE – PII DATA SECURITY

Brian Scott, CIO, Experient, Inc. – Committee Chair

Seth Wilson, Security Project Manager, Experient, Inc.

Julie Baker, VP of Product Development, Map Your Show

Don Kline, CEO, Map Your Show

Ben Behnkendorf, General Manager, Smart City

Bill Charles, CIO, Emerald Expositions

Charles Acquisto, VP of IT, Reed Exhibitions

Bobby Hoffman, Manager, Event Data and Technology, Association of Equipment Manufacturers

Ramon Castro, VP of Technology, a2z, Inc.

STAFF LIAISONS:

Scott Stanton, CEM, CAE, Chief Financial Officer

Jodi Yauch, IT Administrator

RESOURCES

Federal Trade Commission – Data Security
https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

Federal Trade Commission – Protecting Personal Information: A Guide for Business
https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

PCI Security Standards Council – The Prioritized Approach to Pursue PCI DSS Compliance
https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

Common Payment Card Security Myths Dispelled
https://usa.visa.com/dam/VCOM/download/merchants/HU2013Fall-PaymentCardSecurityMythsDispelled.pdf

IAEE
Exhibitions and Events Mean Business
www.iaee.com

International Association of Exhibitions and Events™
12700 Park Central Dr., Ste. 308
Dallas, TX 75251 USA
www.iaee.com • info@iaee.com • +1 (972) 458-8002

LEGAL DISCLAIMER: *Nothing in this document shall be construed to constitute legal advice. In all cases, organizations should see guidance from their own legal counsel and technology professionals.*