BRINGING CYBERSECURITY TO GXP SYSTEMS

Jason Nathaniel Young and John Patterson

Recent cyberattacks like WannaCry and Petya have affected GxP computerized systems, prompting questions on how to address risk from cyberspace using traditional computerized systems validation according to GAMP® 5. This article explores life cycle management of GxP computerized systems and associated cybersecurity risks that can affect patient safety.

Look at any ISPE conference around the world and you'll see that interest in cybersecurity has increased significantly. Unfortunately, confusion and misinterpretation have also accompanied this growth. To discuss cybersecurity issues properly, let's start with a quick overview of what cybersecurity is and how it is implemented.

Cybersecurity is a set of actions taken by stakeholders to reduce risk to systems and information in cyberspace. These actions combine all aspects of information security to address needs for confidentiality, integrity, and availability (known as the "CIA triad") with critical information infrastructure protections.

In the context of protecting GxP-regulated computerized systems, cybersecurity is a method of applying technical and procedural controls to reduce risk to both systems and patient safety. This is accomplished in two ways: identifying and addressing system vulnerabilities and data integrity threats, and providing traceability to established frameworks and technical controls for computerized systems validation (CSV) and corrective and preventive action (CAPA). These activities are implemented via an information security management system (ISMS),* which operates according to established cybersecurity frameworks as well as internal company policies and procedures.

The ISMS becomes a separate organization, built on standard cyber-security roles and responsibilities, that is tasked with enforcing information security governance. The ISMS includes positions such as:

- Chief information security officer
- Information security officer
- Information security manager
- Information system security office

To ensure proper separation of duties, these positions may be imbedded within information technology (IT) governance, but they must be independent of it, and not part of IT management. This is a crucial element of the ISMS, as the purpose of security—whether it be a management or governance position—is to verify that the security configuration is set as directed by the organization's policies and procedures. These established roles and responsibilities rely on methodologies for the implementation of cybersecurity using concepts like defense in depth to manage cybersecurity centrally from within the enterprise. Simply put, "defense in depth" means that security controls increase with each layer of an organization's architecture that provides security to systems. This basic concept is to be maintained when managing the security aspects of standardization, configuration management, and vulnerability/threat monitoring.

This holistic view can make implementing cybersecurity within GAMP 5 guidelines challenging, because centralized production systems in any industry become problematic due to the individual nature of cybersecurity control requirements.

Because cybersecurity personnel are trained to work in specific ways, corporate cultural differences can create friction between the quality unit and ISMS. GAMP 5 terminology and systems-validation methods can conflict with International Organization for Standardization (ISO) and ISACA† definitions and lead to miscommunication. Quality units in other industries and government organizations use the ISMS to verify technical and cybersecurity controls within their validation process according to ISO and ISACA frameworks. No one from a US government quality unit, for example, would have administrative access to a system that was being qualified within their system. That quality unit would request this from the cybersecurity personnel who were qualifying the system.

Within the life sciences, the quality unit ensures that GAMP 5 security procedures for GxP-regulated systems are followed. This is important because regulators increasingly emphasize how and where cybersecurity controls are implemented for both GxP-regulated systems and their associated infrastructures. Questions also arise about how the quality unit should manage and implement cybersecurity controls with its CSV processes.

Since 2008, GAMP 5 has relied on the US National Institute of Standards and Technology (NIST) and ISO standards. More recent cybersecurity methods, however, are much more complex. We frequently see the confusion that arises from this complexity in discussion groups formed during our cybersecurity training.

Here are some sample questions about the organizational structure of the quality management system (QMS) and how ISMS operations can integrate their processes:

- From a cybersecurity perspective, what is the role of the ISMS representative for crafting policies and procedures on GxP-regulated systems within the QMS?

* A systematic approach that applies risk-management procedures to protect sensitive information, people, processes, and IT systems. Frameworks include ISO/IEC 27001, ISACA's COBIT 5, and NIST 800-53.

† Previously known as the Information Systems Audit and Control Association, ISACA—which now goes by its acronym only—is a nonprofit global association for the development, adoption, and use of globally accepted knowledge and practices for information systems.

- How should duties be divided between the quality unit, ISMS members who perform security-related verifications, and the IT department?
- How should risk to GxP-regulated systems from GAMP category 1 (infrastructure) systems be addressed?
- How should threat and vulnerability management be performed? More specifically, how would common vulnerabilities and exposures be used within the CAPA process to track and resolve high-level threats and vulnerabilities?

Other questions focus on areas within the CSV process that need clarification:

- Considering traditional ways of using GAMP categories 1, 3, 4, and 5, how should the system address impact, security categories, and data classification during the initial risk assessment?
- How should cybersecurity requirements that do and do not affect data integrity be defined?
- When using frameworks like ISO/IEC 27001 or COBIT 5, how can traceability to cybersecurity controls be used against GAMP 5 and regulations like CFR 21 Part 11?
- How can standards for cybersecurity technical controls like the Center for Internet Security‡ benchmarks or the Cloud Security Alliance‡ be used for traceability to technical controls?
- What testing methods or best practices can be used during operational qualification and installation qualification?

These are important areas that need consensus on how to deal with them and their effects on qualifying systems.

COLLABORATION

Fortunately, Chris Reid, a member of the ISPE Leadership Team, has announced a new collaboration between ISPE and ISACA to create cybersecurity guidance for the industry. This effort is supported by the highest levels of ISPE leadership. Discussions are expected to yield guidance from ISACA to the cybersecurity community and from ISPE to the quality unit.

With this in mind, the cybersecurity community for GxP-relevant systems believes that guidance should address roles and responsibilities as well as traceability methods for cybersecurity technical controls. The payment card industry (PCI), for example, uses the PCI Data Security Standard (PCI DSS), which issues guidance for a range of organizations—from Walmart to local restaurants—on their responsibilities for payment-system cybersecurity. One requirement is the need for penetration testing. The PCI provides detailed guidance on testing, methods, scope, time frames, and reporting mechanisms. ISPE may want to consider some of these methods and concepts when crafting its new guidance.

ISMS SUPPORT TO GXP COMPUTERIZED SYSTEMS

To see why clear roles and responsibilities are important, let's look at the responsibilities for one of the roles we identified earlier: the chief information security officer, or CISO.

‡ Center for Internet Security: A nonprofit organization that provides cyber-threat prevention, protection, response, and recovery for US government entities.

‡ Cloud Security Alliance: A nonprofit organization that offers cloud security research, education, certification, events, and products, working in collaboration with industry, higher education, and government on a global basis.

TABLE A: ACRONYMS AND INITIALISMS

CAPA	Corrective and preventive action
CFR	US Code of Federal Regulations
CIA	Confidentiality, integrity and availability
CISO	Chief information security officer
CSV	Computerized systems validation
DAR	Data at rest
EU	European Union
GAMP®	Good automated manufacturing practices
GDPR	General data protection regulation
GxP	Good "x" practices
ISMS	Information security management system
ISO	International Organization for Standardization
ISACA	Previously known as the Information Systems Audit and Control Association
ISPE	International Society for Pharmaceutical Engineering
IT	Information technology
NIST	National Institute for Standards and Technology
PCI	Payment card industry
PCI-DSS	PCI Data Security Standard
PII	Personally identifiable information
QMS	Quality management system
SC	Security category

According to ISACA, the CISO is responsible for the enterprise information security program and, more specifically, for ensuring that the ISMS is established and maintained according to the company's strategic cybersecurity plan. A key component of the CISO role is creating a structure to support the QMS. The CISO must also ensure that the governance portion of the ISMS—which supports the QMS—does not conflict with the information security manager's mandate to enforce company security policies and procedures. The CISO must also balance cybersecurity needs throughout the organization, including infrastructure and GxP-regulated systems. To accomplish all of this, the strategic plan must include separation of duties and be scalable to the size of the organization.

According to ISACA, the ISMS must align, plan, organize, and manage the following areas, some of which play a significant role within the QMS:

- IT management framework
- Strategy
- Enterprise architecture
- Innovation
- Portfolio
- Budget and costs

- Human resources
- Relationships
- Service agreements
- Suppliers
- Quality
- Risk
- Security

Ensuring that cybersecurity policies and procedures are addressed within the QMS is important, because they play a role in determining the organization's overall risk. One way to address issues related to GxP-regulated systems and ISMS is to establish an information security officer (or other governance position) to support QMS security functions. The data steward from the *GAMP Records and Data Integrity Guide* would be an excellent choice for this job function.

As the ISMS is responsible for the cybersecurity posture of the infrastructure, it must also define the process for addressing risk from the infrastructure to GxP-regulated systems (and vice versa). Critically important areas are logging, monitoring, architecture, and access control, because each of these items directly affects production systems that require services from the infrastructure. Many can be done through documented procedures, others may require specific methods for defining requirements and testing during the CSV process.

In addition to infrastructure, another key component is how the ISMS manages threats and vulnerabilities. Those that affect data integrity for GxP-regulated systems should have a defined method for inclusion to CAPAs. Most ISMS operations actively monitor their local computer emergency response team for alerts and bulletins, and document findings from security devices like vulnerability-scanning software, which use traceability for tracking and remediation.

CYBERSECURITY CONTROLS AND TESTING

Beyond the issues of roles and responsibilities, there are other areas where guidance from ISPE could help improve cybersecurity. These are mostly technical, but a few procedural examples exist as well. When addressing cybersecurity risks, the most important part of the process is during the initial risk assessment. This is when the system security category (SC) should be established to determine technical controls and testing methods that will be used. The SC is based on a combination of items such as data classification, asset valuation, threat modeling, and system impact. Decisions about internal policies and procedures should also be made during the initial risk assessment because this determines the security controls that will be applied. NIST recommends using the highest level of the impact on any one area of CIA to determine an SC:

SC = {(confidentiality, impact), (integrity, impact), (availability, impact)}

where the acceptable values for potential impact are low, medium, or high.

This is different from traditional GxP testing based on GAMP categories 3, 4, and 5. When looking at cybersecurity risks, all systems are tested according to the computerized system security category defined during the initial risk assessment. Benchmarks like those from the Center for Internet Security incorporate this methodology, providing different levels of security controls.

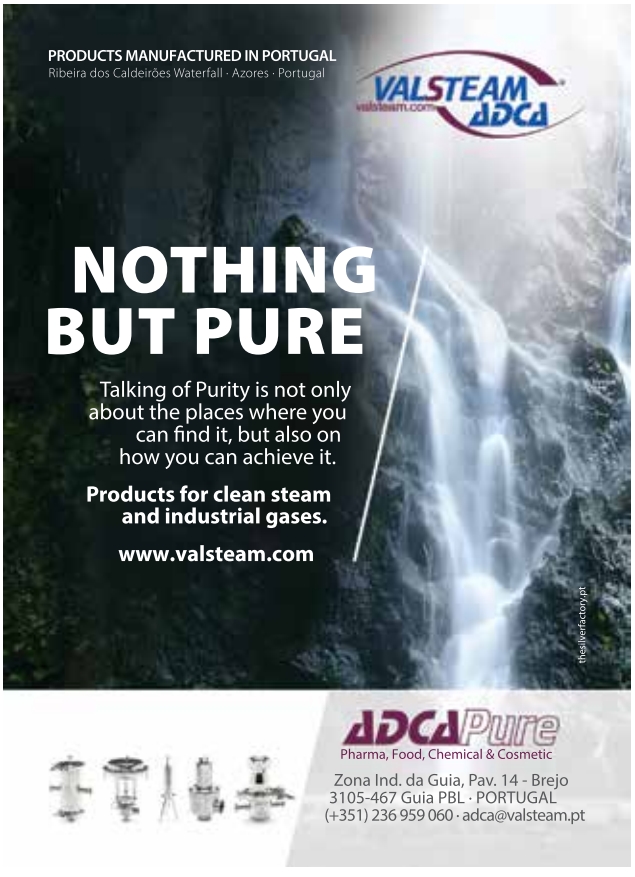
Once the SC is established, it can be used to create templates to apply appropriate cybersecurity controls to data integrity issues. Guidance from ISPE and ISACA will be especially valuable in this area. Establishing how the quality unit should determine technical or procedural cybersecurity will take time and coordination with the ISMS, because many of these controls will be provided within the protection of the infrastructure. It's helpful to avoid duplication of work at this step, and to reference cybersecurity controls.

PII

Another consideration is the need to safeguard personally identifiable information (PII) in any system that processes it. Here, guidance from ISPE and ISACA based on typical situations could help reduce the amount of work required to create these methods for each organization.

Using encryption to protect data at rest (DAR) or in transit shows how portions will be provided by the infrastructure, depending on the situation. A portable system that contains PII and is GxP regulated, for example, must be protected by DAR encryption. This type of control, which is designed to protect data privacy and integrity, is usually provided by an infrastructure service—such as Microsoft's BitLocker, for example.

When considering data privacy for GxP-relevant systems, quality unit personnel can benefit greatly from cybersecurity professionals, as they are well versed in regulations like the European Union's (EU) General Data



GUIDANCE FROM ISPE COULD HELP IMPROVE CYBERSECURITY

Protection Regulation (GDPR), and have reporting mechanisms that allow companies to notify the EU of data breaches or compromised systems within 72 hours. This is important because the GDPR authorizes financial penalties of up to €20 million or 4% of annual worldwide turnover, whichever is greater.

In addition to controls identified within specifications documents, their associated qualifications could also benefit from ISPE cybersecurity testing guidance. At what stages, for example, and under what conditions should a penetration test or a simple vulnerability scan be performed? The PCI DSS standard provides explicit guidance on how and when penetration tests are to be accomplished, and could be instructive for application within a GxP environment. Any system that is publicly accessible via the internet, for example, should have a penetration test performed yearly. Other systems, depending on their functionality, makeup, and placement within a network may not require such costly and extensive evaluation. Creating test methods within qualifications will take the most work, as they are highly technical, but they will be the easiest problems to solve once the roles and responsibilities have been addressed.

Finally, a realistic view of risk assessment and risk acceptance can be summed up by the IT aphorism "garbage in, garbage out." If security gaps persist throughout a validation, it is natural to assume that neither GxP- nor non-GxP-relevant cybersecurity are included in the system risk assessment. This is not only incorrect, but it provides a false sense of security.

Much work must be done within the risk assessment to assign appropriate levels of risk to the cybersecurity requirements for other GxP controls, such as data integrity and risk acceptance or mitigation. How these controls affect CAPA and incident response should be explored as well. What time frame should be allowed to correct these types of problems? Who oversees the remediation? This will be true for all zero day[§] exploits that affect the confidentiality of any given process.

SUMMARY

As cybersecurity threats increase in frequency and intensity, it is important that organizations like ISPE continually improve their guidance to address such risks. Collaboration between ISACA and ISPE will be a big step forward in understanding many of the challenges that face the life sciences community. As security professionals, our goal is to enhance GAMP 5, clarify the ISMS role within the process, and address risks to GxP-relevant systems and data in a much more inclusive manner. ‹›

[§] Zero day: an unknown software vulnerability; code used to exploit this vulnerability

References

1. EUR-Lex. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). 27 April 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG
2. European Commission. Health and Consumers Directorate-General. EudraLex, "The Rules Governing Medicinal Products in the European Union." Volume 4, "Good Manufacturing Practice Medicinal Products for Human and Veterinary Use." Annex 11, "Computerised Systems." 30 June 2011. https://ec.europa.eu/health//sites/health/files/files/eudralex/vol-4/annex11_01-2011_en.pdf
3. International Organization for Standardization. ISO/IEC 27001:2013. "Information Technology – Security Techniques – Information Security Management Systems – Requirements." October 2013. https://www.iso.org/standard/54534.html
4. ISACA. COBIT 5. https://cobitonline.isaca.org
5. International Society for Pharmaceutical Engineering. *GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems*. February 2008. https://ispe.org/publications/guidance-documents/gamp-5
6. ———. *GAMP Good Practice Guide: Testing GxP Systems.* 2nd ed. December 2012. https://ispe.org/publications/guidance-documents/gamp-testing-gxp-systems
7. ———. *GAMP Good Practice Guide: Global Information Systems Control & Compliance.* 2nd ed. February 2017. https://ispe.org/publications/guidance-documents/gamp-global-information-systems-compliance
8. ———. *GAMP Guide: Records and Data Integrity.* March 2017. https://ispe.org/publications/guidance-documents/gamp-records-pharmaceutical-data-integrity
9. US National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." Version 1.0. 12 February 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
10. ———. NIST Special Publication 800-53, Revision 4. *Security and Privacy Controls for Federal Information Systems and Organizations.* April 2013. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
11. Palmer, E. "Still Reeling from Cyberattack, Merck Warns Some Drug Supplies May Be Delayed." *FiercePharma*, 28 July 2017. https://www.fiercepharma.com/pharma/merck-production-r-d-still-recovering-from-cyber-attack-but-still-outperforms
12. Payment Card Industry. Security Standards Council. Data Security Standard (DSS) 11.3. "Information Supplement: Requirement 11.3 Penetration Testing." 15 April 2008. https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf
13. Pharmaceutical Inspection Co-Operation Scheme. "Guide to Good Manufacturing Practice for Medicinal Products (Part II)." 22 May 2015. https://www.picscheme.org/layout/document.php?id=977
14. Shaban, H., and E. Nakashima. "Pharmaceutical Giant Rocked by Ransomware Attack." *Washington Post,* 27 June 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/06/27/pharmaceutical-giant-rocked-by-ransomware-attack/?utm_term=.92fe9b3e3788
15. US Food and Drug Administration. Federal Food, Drug, and Cosmetic Act (FD&C Act). https://www.fda.gov/RegulatoryInformation/LawsEnforcedbyFDA/FederalFoodDrugandCosmeticActFDCAct/default.htm
16. US Food and Drug Administration. Code of Federal Regulations. Title 21, Chapter I, Subchapter A, Part 11: Electronic Records; Electronic Signatures. 1 April 2017. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1

About the authors

Jason N. Young is the CEO of Silver Bullet Security and has worked within the cyber security field for more than 15 years. Currently he is pursuing his doctorate at Deakin University in Australia, focused on the integration of cyber security to GxP Processes for the pharmaceutical industry. He began his career in information security while serving in the US military until he reached the position of information assurance manager for US Africa Command. At that point Jason began working in the life sciences industry as a cyber security architect. using his background in cyber security implementation to build secure architectures. He has also authored two publications for the SANS Institute, with certifications from SANS, ISC2, and NSA. With a background mostly in network security operations, Jason has also worked collaboratively on creating the US Army Europe's courseware for information assurance and computer network defense. He has been an ISPE member since 2014.

John Patterson is CISO & Head of Business Technology Governance for Merck KGaA, Darmstadt, Germany. Mr Patterson is based in the USA, and is part of EMD Serono, a US affiliate in Merck KGaA's biopharmaceutical business. Mr. Patterson is responsible for data governance, information security & protection, IT GxP inspection readiness and overall IT compliance within the global Merck KGaA information technology organization. John possesses over 30 years' experience in biochemical process engineering, chemical and biopharmaceutical manufacturing, information technology and, most recently, information security and IT regulatory compliance. He earned an MS in engineering from Purdue University and a BS in agricultural engineering from the University of Wisconsin–Madison. An ISPE member since 2005, he has been a contributing author to various publications in pharmaceutical design engineering, computer process validation, and pharmaceutical risk management.