INFORMATION SECURITY IS PRACTICED LIKE EARLY MEDICINE:

How to Standardize, Test and Deliver Trust in the Profession

KEY ISSUE:

While information security is under greater scrutiny from the boardroom, what business leaders see behind the curtain is frightening. As an industry, security teams most often operate in isolation, not receiving transparent, reliable data about the experiences of others.

What senior business managers quickly realize, and what security leaders already know, is that the current approach used in information security is characteristic a relatively young science. Our adversaries demand that we move faster.

The pace of organizational innovation in security is not advanced compared to other managerial disciplines that take advantage of shared academic research and tribal knowledge. Throughout the profession, pockets of innovation exist, but these innovations are not uniformly deployed to the field.

The incubation period of discovery can be accelerated. The evolution of medicine from the 18th to the 19th century demonstrated that broad advances can occur through an experimental approach and reliable reporting.

What allowed the blossoming of two hundred years of discovery into broad impact was that technology advances were tested with trusted standards, shared with a trusted community and then deployed through trusted institutions.[1]

CHALLENGES AND OPPORTUNITIES:

The state of information security art

RIGHT NOW

There are positive signs that security leaders are curious about sharing insight about their efforts, but there are still barriers to sharing, and strategy development is rarely based on experimentation or widely available case studies.

- CISOs currently use industry surveys to gain insight for benchmarking, instead of transparent and standardized reporting by a broad set of companies. This approach is the best we can do in many cases, but security teams are left to decipher the relevance of the survey population and the questions. These surveys are usually annual and seldom report consistent data sets over time.

BACK THEN

The development of medicine between the 17th and 19th centuries teaches us that the following criteria help aid the development of a young science:

1. Infrastructure created for reporting on highly consistent basis.

2. Technological breakthroughs focused on better examination and diagnosis.
3. Rigorous professional criteria provided the ability to be selective about candidates.
4. Professional bodies emerged, both academic and professional, to enforce practice standardization.
5. Accepted standards of experimentation were established.
6. Experimentation and practical implementation were fused through co-housing the functions at teaching hospitals.
7. Specializations were clearly defined.
8. Community health became a major concern.

These criteria were met for medicine through the following stages. These serve as discussion points for how information security may also develop.

- **Data reporting:** By the end of the 17th century, an emerging reporting infrastructure revealed in what areas of London people were dying the most from outbreaks of the plague. In 1661, a non-medical tradesman named John Graunt took this weekly data and provided analysis of it, eventually leading to the creation of insurance actuarial tables in 1669. [2] [3]
- **Technological breakthrough:** The 17th and 18th century also saw technological advancement in terms of the microscope and microbiology, immunization, and in the autopsies. Technology advances in microscopy started in the 17th century. [4] [5] [6] In the 19th century, advances in anesthesia and the discovery of germs as the causes of disease further transformed the practice of healthcare. [7]
- **Professional criteria enhanced:** While America was held back in clinical advancement because it lacked advanced medical schools in the 17th century, by the 19th century medical schools at Harvard University, Lind University in Chicago, and Johns Hopkins University all set higher entrance requirements and longer school years, raising professionalization and leading to advances in microscopy and bacteriology. [8] [9]
- **Experimentation standards:** Claude Bernard established himself as a founder of experimental physiology, and medical experimentation in general with his Study in Experimental Medicine in 1865. [10] [11]
- **Theory fused with practice:** 19th century medicine made leaps in marrying practice and experimentation through the use of teaching hospitals, first in France, then in Britain and Germany. [12] [13]
- **Specializations:** Clinicians of all kinds had undertaken debate to delineate those qualified to practice and those who were not. This debate focused on the spectrum of clinical practice types (surgery, chiropractic, etc.), and then within the hierarchy of each individual practice (those with a shorter period of formal education). Medical specializations started to develop in the 19th century because the body of knowledge became too great. Surgery was established as distinct from general practice. Scientists focused on distinct systems such as disease and the nursing system. On the hierarchy side, nursing developed as a distinct practice of care to aid physicians, thanks to the help of leaders like Florence Nightingale.[14] [15]
- **Community and population health:** Sanitation was the initial impetus for community health, with the introduction of bathrooms by John Harrington in the 16th century. The use of vaccinations for small pox by the end of the 18th century also advanced community health. Community health became even more important as the industrial revolution emerged, placing large numbers of people together in cramped factories throughout the 19th century, taxing community health support systems. The 1850s saw dramatic improvements in community health, with Lemual Shattuck formally introducing community health needs in Massachusetts, and John Snow in London who removed the handle of a water pump to reduce cholera cases. [16] [17]

THE PATH FORWARD:

Standardized reporting, specialized disciplines

The information security community needs to enhance its ability to practically leverage the science developed over the last decades to inform strategy. **These seven key aspects of medical science evolution can also be applied to security strategy development.**

- **Data reporting:** The reporting of mortality tables in London was driven by various rulers due to the outbreak of plague, but was executed through parishes by an order of monks. Information security would benefit from the development of standardized incident reporting.

A combination of state need, executed by a trusted and dedicated third party through already existing infrastructure (in this example, monks at parishes) provides a blueprint for this concept.

- **Technological breakthrough:** Technological breakthroughs must continue to happen through a robust encouragement of those who are pushing the boundaries in our field. This is a strong point in certain parts of the industry, and it outpaces our ability to learn how to maximize the use of the technology. Security strategy developers should recognize this and create implementation expectations accordingly.
- **Professional criteria enhanced:** Certification bodies could become more selective and possibly require more explicit proof of an apprenticeship program. Degree programs should continue to build their information security degrees as a unique discipline within computer science with distinct strategic objectives.
- **Experimentation standards:** Security strategies should be tested through the use of comparative and detailed case studies. Enterprises that pursue different strategies should be examined for performance.
- **Theory fused with practice:** Information security strategy developers should be exposed to many different security success and failure stories, as well as spend time with various security teams as they implement new strategy objectives.
- **Specializations:** Security strategy specialization should emerge around the security program with the ability to credibly explain why certain strategies should be pursued in certain situations.
- **Community and population health:** Security leaders should be open and transparent with each other about their successes and failures whenever possible, and also pave the way through strategy to share intelligence with trusted parties.

Heath Nieddu
Senior Research Analyst
Solutions Research and Development Optiv

Jason Clark
Chief Strategy and Security Officer Optiv

1 Federal Trade Commission. "Internet of Things: Privacy and Security in a Connected World." January, 27 2015. p. i. Retrieved from: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
2 Lyons, Albert S. "17th Century Medicine" Health Guidance, Retrieved from: http://www.healthguidance.org/entry/6350/1/Medical-History--The-Seventeenth-Century.html
3 Ed, Stephan. "A Life of John Graunt" Retrieved from: http://www.edstephan.org/Graunt/grauntbio.html
4 Lyons, Albert S. "17th Century Medicine" Health Guidance, Retrieved from: http://www.healthguidance.org/ntry/6350/1/Medical-History--The-Seventeenth-Century.html
5 Retrieved from: http://www.history-of-the-microscope.org/anton-van-leeuwenhoek-microscope-history.php
6 Stern, Alexandra Minna and Markel, Howard. "The History of Vaccines and Immunization: Familiar Patterns, New Challenges." Health Affairs, May 2005. Pp.611-621 Retrieved from: http://content.healthaffairs.org/content/24/3/611.full
7 Lyons, Albert S. "17th Century Medicine" Health Guidance, Retrieved from: http://www.healthguidance.org/entry/6350/1/Medical-History--The-Seventeenth-Century.html
8 Lyons, Albert S. Specializations developed because the volume of data was too great.
9 Porter, Roy (1999) [1997]. The Greatest Benefit to Mankind: A Medical History of Humanity from Antiquity to the Present. New York: W. W. Norton & Company. p. 316–317.
10 Wise, Peter, Retrieved from: http://www.claude-bernard.co.uk/page2.htm
11 Lyons, Albert S. 19th Century Medicine
12 Lyons, Albert S. Specializations developed because the volume of data was too great. p.46
13Mckee, Martin and Healy, Judith. "Hospitals in a Changing Europe." Open University Press. Buchinkham p. 35. Retrieved from: http://www.euro.who.int/__data/assets/pdf_file/0004/98401/E74486.pdf
14 Lyons, Albert S. Specializations developed because the volume of data was too great. p.46
15 Nightingale, Florence. "Notes on Nursing: what it is and what it is not." JB Lippencott Co., Philadelphia. 1859.
16 Green, Lawrence W., Mckenzie, James F. "Community Health." Encyclopedia of Public Health. 2002. Retrieved from: http://www.encyclopedia.com/topic/Community_Health.aspx
17 Lyons, Albert S. 19th Century Medicine

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

4.16 | F3