

**FITLSDOG**



# **FITLSDOG**

**The Financial Information Technology  
Leader's Strategy Development and  
Operations Guide**

Anthony Scarola

Security Connect LLC

Copyright © 2024 by Security Connect LLC. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the copyright holder, except for brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

For permission requests, email the publisher, Security Connect LLC, at [info@securityconnect.us](mailto:info@securityconnect.us) with the subject line “Attention: Permissions Coordinator.”

First Edition, 2024

ISBN: 979-8-874-21644-3

Library of Congress Control Number: 2024906187

**Limit of Liability/Disclaimer of Warranty:** While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties concerning the accuracy or completeness of the contents of this book and expressly disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when it was written and when it was read. Neither the publisher nor the authors shall be liable for any loss of profit or other commercial damages, including but not limited to special, incidental, consequential, or other damages.

If you believe you have found a mistake in this book, please bring it to our attention by emailing us at [info@securityconnect.us](mailto:info@securityconnect.us).

Cover design: OpenAI DALL-E

Printed in the United States of America

# References

- Aldas-Manzano, J., Ruiz-Mafe, C., Sanz-Blas, S., & Lassala-Navarre, C. (2011). Internet banking loyalty: evaluating the role of trust, satisfaction, perceived risk and frequency of use. *The Service Industries Journal*, 31(7), 1165-1190.
- Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: an analysis of the literature. *Journal of Decision Systems*, 25(sup1), 64-75.
- American Bankers Association. (2012, January 17). Convenient, but how secure? *The New York Times*, p. A22.  
<https://www.nytimes.com/2012/01/17/opinion/banking-online-is-convenient-but-how-secure.html>
- Anderson, H. (2012). When does HIPAA apply to banks? BankInfoSecurity.  
<http://www.bankinfosecurity.com/when-does-hipaa-apply-to-banks-a-4386>
- Antón, P. S., Anderson, R. H., Mesic, R., & Scheiern, M. (2003). Finding and fixing vulnerabilities in information systems: The vulnerability assessment & mitigation methodology. RAND; National Defense Research Institute.  
[http://www.rand.org/content/dam/rand/pubs/monograph\\_reports/2005/MR1601.pdf](http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1601.pdf)
- Archer GRC. (n.d.). Retrieved March 22, 2024, from  
<https://www.archerirm.com/content/grc>
- Bacik, S. (2008). *Building an effective information security architecture*. CRC Press.
- Baker, J. B., & Weilz, R. (2008). *Electromagnetic pulse (EMP) attack: A preventable homeland security catastrophe*. The Heritage Foundation.  
<http://www.heritage.org/homeland-security/report/electromagnetic-pulse-emp-attack-preventable-homeland-security-catastrophe>
- Batini, C., & Scannapieco, M. (2016). Data and Information Quality: *Dimensions, Principles and Techniques*. Springer.
- Bazgosha, G., Eizi, N., Nawaser, K., & Parhizgar, M. M. (2012). Technology of e-

- banking: perspective of costumers' perceived risk and uncertainty. *Indian Journal of Science and Technology*, 5(2), 2200-2208.
- Be Supported. (2017, October 17). *Managing complexity in financial services information technology*. Cloud Business.  
<https://cloudbusiness.com/financial-services-information-technology/>
- Beatty, R. C., Arnett, K. P., & Liu, C. (2005). *CIO/CTO Job Roles: An Emerging Organizational Model*. Retrieved August 22, 2021 from California State University San Bernardino ScholarWorks:  
<https://scholarworks.lib.csusb.edu/ciima/vol5/iss2/1>
- Beaumier, C. M. (2006). Multifactor authentication: a blow to identity theft? New guidance from the FFIEC addresses authentication for online banking. *Bank Accounting & Finance*, 19(2), 33-38.
- Blazier, D. (2011). Password plus. *Independent Banker*, 61(11), 74-75.
- Boës, X., Brenet, M., Feibel, C., Harmand, S., Lenoble, A., Lepre, C., . . . Quinn, R. (2015, May 20). 3.3-million-year-old stone tools from Lomekwi 3, West Turkana, Kenya. *Nature*. <https://www.nature.com/articles/nature14464>
- Boyle, M. (2023). Wall street CEOs like Jamie Dimon talk about how going remote 'doesn't work,' but most banks are actually flexible. *Fortune*.  
<https://fortune.com/2023/03/07/remote-work-wall-street-banks-flexible-two-thirds-support-survey-jamie-dimon/>
- Bradford, C. (2015). How the cost of unpatched software figures into HIPAA and industry compliance. *Storagecraft*.  
<http://www.storagecraft.com/blog/unpatched-software-hipaa/>
- Brous, P., Janssen, M., & Krans, R. (2020). Data Governance as Success Factor for Data Science. In *Responsible Design, Implementation and Use of Information and Communication Technology: 19th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2020, Skukuza, South Africa, April 6–8, 2020, Proceedings, Part I* (Vol. 12066, pp. 431–442). [https://doi.org/10.1007/978-3-030-44999-5\\_36](https://doi.org/10.1007/978-3-030-44999-5_36)

- BSM Consulting, Inc. (n.d.). Portrait of an ENFJ: Extraverted intuitive feeling judging. Retrieved December 25, 2023, from <https://www.personalitypage.com/ENFJ.html>
- Carnegie Endowment for International Peace. (n.d.). *Timeline of cyber incidents involving financial institutions*. Retrieved January 21, 2024, from <https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline>
- Chenok, D. (n.d.). *Sharing information: Protecting access* [video]. Center for Strategic and International Studies (CSIS). Retrieved December 25, 2023, from <http://player.vimeo.com/video/46638084>
- Choudhary, V., & Vithayathil, J. (2013). The impact of cloud computing: Should the IT department be organized as a cost center or a profit center? *Journal Of Management Information Systems*, 30(2), 67-100. doi:10.2753/MIS0742-1222300203.
- Cole, G. (2012, October 24). Burlington addressing cyber theft after money drained from account. *Skagit Valley Herald (Mt. Vernon, WA)*.
- Comparison of file sharing applications*. (n.d.). Retrieved March 22, 2024 from Wikipedia:  
[https://en.wikipedia.org/wiki/Comparison\\_of\\_file\\_sharing\\_applications](https://en.wikipedia.org/wiki/Comparison_of_file_sharing_applications)
- Consumer Financial Protection Bureau. (2018). 12 CFR Part 1016 - Privacy of Consumer Financial Information (Regulation P).  
<https://www.consumerfinance.gov/rules-policy/regulations/1016/>
- Cristina, T., Beatrice, C., & Florentina, P. (2008). E-banking – impact, risks, security. *Annals Of The University Of Oradea, Economic Science Series*, 17(4), 1537-1542.
- CSID. (n.d.). [Web site]. Retrieved December 25, 2023, from <https://www.csid.com/>
- Cybersecurity & Infrastructure Security Agency (CISA). (2021, February 1). What is cybersecurity? Retrieved December 26, 2023, from

- <https://www.cisa.gov/news-events/news/what-cybersecurity>  
Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). EMP program status report. <https://www.cisa.gov/resources-tools/resources/emp-program-status-report>
- Dawes, S. S. (2010). Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly*, 27(4), 377-383.
- Deloitte. (n.d.). *Cybersecurity threat trends report 2023*.  
<https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-threat-trends-report-2023.html>
- Deloitte. (n.d.). *Modernizing legacy systems in banking*. Retrieved March 22, 2024, from <https://www2.deloitte.com/us/en/pages/financial-services/articles/modernizing-legacy-systems-in-banking.html>
- Department of Homeland Security (DHS). (2013). *What is critical infrastructure?*  
<https://www.cisa.gov/sites/default/files/publications/ip-fact-sheet-508.pdf>.
- Dockterman, E. (2013, August 26). *Your identity is worth \$5 on the black market*. TIME. <http://newsfeed.time.com/2013/08/26/your-identity-is-worth-5-on-the-black-market/>
- Dulaney, E., & Harwood, M. (2012). *CompTIA Network+ N10-005 Authorized Exam Cram: Fourth Edition*. Indianapolis, IN: Pearson IT Certification.
- EC-Council. (2010). *Ethical hacking and countermeasures: Linux, macintosh, and mobile systems*. Cengage Learning.
- EC-Council. (2010). *Ethical hacking and countermeasures: Web applications and data servers*. Cengage Learning.
- EC-Council. (2016). *Ethical hacking and countermeasures: Threats and defense mechanisms*. Cengage Learning.
- Edmondson, N. (2012, June 27). Operation high roller: \$78m global financial fraud ring uncovered. *International Business Times*.  
<https://www.ibtimes.co.uk/operation-high-roller-global-fraud-ring-macafee-356892>



- European Network and Information Security Agency (ENISA). (2012, December 12). Introduction to return on security investment: Helping CERTs assessing the cost of (lack of) security.  
[https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at\\_download/fullReport](https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport)
- Federal Deposit Insurance Corporation (FDIC). (2020, May 15). What we do.  
<https://www.fdic.gov/about/what-we-do/index.html>
- Federal Deposit Insurance Corporation (FDIC). (2021, September 14). Laws & regulations: Important banking laws.  
<https://www.fdic.gov/resources/regulations/important-banking-laws/index.html>
- Federal Deposit Insurance Corporation (FDIC). 12 CFR Part 363: Annual independent audits and reporting requirements.  
[http://ithandbook.ffiec.gov/media/21953/fdi-12cfr363-annual\\_independ\\_audit\\_report\\_requir.pdf](http://ithandbook.ffiec.gov/media/21953/fdi-12cfr363-annual_independ_audit_report_requir.pdf)
- Federal Financial Institutions Examination Council (FFIEC). (2006). Releases guidance on internet banking authentication. Point for Credit Union Research & Advice, 15.
- Federal Financial Institutions Examination Council (FFIEC). (2014, November 3). FFIEC releases cybersecurity assessment observations, recommends participation in financial services information sharing and analysis center.  
<http://www.ffiec.gov/press/pr110314.htm>
- Federal Financial Institutions Examination Council (FFIEC). (2015). Information technology (IT) examination handbook: Management.  
<https://ithandbook.ffiec.gov/it-booklets/management/>
- Federal Financial Institutions Examination Council (FFIEC). (2015). Cybersecurity assessment tool. <https://www.ffiec.gov/cyberassessmenttool.htm>
- Federal Financial Institutions Examination Council (FFIEC). (2022). Cybersecurity resource guide for financial institutions.

<https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf>

Federal Financial Institutions Examination Council (FFIEC). (n.d.). Information technology (IT) examination HandBook InfoBase.

<https://ithandbook.ffiec.gov/>

Federal Reserve Board (FRB). (n.d.). *12 CFR Part 208, Appendix D-1: Interagency guidelines establishing standards for safety and soundness.*

[http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard\\_customer\\_info\\_final\\_rule-010201.pdf](http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf)

Federal Reserve System. (2020, December 18). *Large Financial Institutions.*

<https://www.federalreserve.gov/supervisionreg/large-financial-institutions.htm>

Fenrich, K. (2008). Securing your control system: the ‘CIA triad’ is a widely used benchmark for evaluating information system security effectiveness. *Power Engineering*, (2). 44.

Filshinskiy, S. (2013). Cybercrime, cyberweapons, cyber wars: Is there too much of it in the air?. *Communications Of The ACM*, 56(6), 28-30.

doi:10.1145/2461256.2461266.

<https://dl.acm.org/doi/10.1145/2461256.2461266>

Financial Services Information Sharing and Analysis Center. (2012). *FS-ISAC announces the results of account takeover survey.* Retrieved June 14, 2012,

from

<http://www.aba.com/Solutions/Fraud/Documents/FSISACPressRelease62012.pdf>

Florina, V., Liliana, M., & Viorica, I. (2008). Risk management of e-banking activities. *Annals Of The University Of Oradea, Economic Science Series*, 17(3), 878-881.

Ganpat, S. (2014, June 4). *How large an IT staff do you need: Is there a standard ratio of IT staff to total employees?* Intersect.

- <https://www.interxect.com/how-large-an-it-staff-do-you-need/>
- Gartner, Inc. (2021). IT Glossary: Data Lifecycle Management.
- Gelles, M. G., Mahoutchian, T., & Deloitte Consulting. (2012). Mitigating the insider threat: Building a secure workforce. *NIST*.  
<https://csrc.nist.gov/presentations/2012/mitigating-the-insider-threat-building-a-secure>
- Gibson, D. (2012). *SSCP systems security certified practitioner: All-in-one exam guide*. B. E. Rogers (Ed.). New York, NY: McGraw-Hill.
- Gonza, E. (2020, November 18). *PRINCE2 implementation at the central bank of Uganda*. Axelos. <https://www.axelos.com/resource-hub/case-study/prince2-implementation-at-central-bank-of-uganda>
- Gramm-Leach-Bliley Act. (2014). *Title V – Privacy*.  
<http://www.fdic.gov/regulations/laws/rules/8000-4000.html>
- Greenwald, G. (2010, June 18). The strange and consequential case of Bradley Manning, Adrian Lamo and WikiLeaks. *Salon*. Retrieved January 17, 2022, from [https://www.salon.com/2010/06/18/wikileaks\\_3/](https://www.salon.com/2010/06/18/wikileaks_3/)
- Greenwald, J. (2014). Cybersecurity framework unveiled; NIST rules help firms contend with breaches. *Business Insurance*, (5).
- Gregg, M. (2005). CISSP security-management practices. *Pearson Education*. Retrieved March 22, 2024, from <https://www.pearsonitcertification.com/articles/article.aspx?p=418007&seqNum=6>
- Grennan, J. (2022, April 12). *FinTech Regulation in the United States: Past, Present, and Future*. The FinReg Blog.  
<https://sites.duke.edu/thefinregblog/2022/04/12/fintech-regulation-in-the-united-states-past-present-and-future/>
- GTB Technologies. (n.d.) *Case study: Global financial institution delivers compliance to GDPR & other regulations including CCPA*. GTB Technologies. Retrieved March 22, 2024, from <https://gttb.com/compliance->

regulatory-requirements/global-financial-institution-delivers-compliance-to-gdpr-and-ccpa/

Heath Insurance Portability and Accountability Act. (2014). *Understanding Health Information Privacy*. Retrieved May 12, 2015, from

<https://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>

Heggesteun, J. (2013). Target's data breach nightmare reveals the vulnerability of traditional point-of-sale systems. Business Insider.

<https://www.businessinsider.com/analysis-of-target-data-breach-2013-12>

Henderson, D. (2014, February 12). Big data demands more than commodity hardware. InfoWorld. <https://www.infoworld.com/article/2610477/big-data/big-data-demands-more-than-commodity-hardware.html>

Hipsher, A. K., & Sullivan, C. D. (2012). PCI compliance: The risks banks can miss. <https://www.banktech.com/compliance/pci-compliance-the-risks-banks-can-miss/a/d-id/1295190.html>

Howard, R. (2023). *Cybersecurity first principles: A reboot of strategy & tactics*. Wiley.

Ingram Micro. (2015, March 5). Understanding Big Data, Forensics, and Information Security. Ingram Micro Advisor. Retrieved April 14, 2016, from <http://www.ingrammicroadvisor.com/data-center/understanding-big-data-forensics-and-information-security>

Internet Crime Complaint Center. (2023). *2023 internet crime report*. Federal Bureau of Investigation.

[https://www.ic3.gov/Media/PDF/AnnualReport/2023\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf)

Internet Crime Complaint Center. (n.d.). *Fraud advisory for businesses: Corporate account take over*. Retrieved October 23, 2012, from

<https://www.ic3.gov/media/2010/corporateaccounttakeover.pdf>

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing (NIST SP-800-144).

<https://csrc.nist.gov/pubs/sp/800/144/final>

- Kean, R., Harris, D., Meegan, J., Pardee, B., Le Roux, Y., Dotson, C., ..., Cohen, E. (2012). Security for cloud computing: 10 steps to ensure success. Retrieved March 17, 2013, from [http://www.cloud-council.org/Security\\_for\\_Cloud\\_Computing-Final\\_080912.pdf](http://www.cloud-council.org/Security_for_Cloud_Computing-Final_080912.pdf)
- Kocieniewski, D. (1999, April 3). *Melissa virus suspect caught*. The New York Times. Retrieved December 26, 2023, from <https://archive.nytimes.com/www.nytimes.com/library/tech/99/04/biztech/articles/03melissa.html>
- Korora, A. M. (2013). "Social engineering." Salem Press Encyclopedia Research Starters. *EBSCOhost*.
- Koster, J. (2011). 5 basic steps your financial institution needs to take to be compliant with increased standards in internet banking. *Connecticut Banking*, 6-7.
- Krebs, B. (2013, June). *FDIC: 2011 FIS Breach Worse Than Reported*. Retrieved from Krebs on Security: <https://krebsonsecurity.com/2013/06/fdic-2011-fis-breach-worse-than-reported/>
- Krutz, R., and Vines, R. D. (2007). *The CISSP and CAP prep guide: platinum edition*. White Plains, NY: Wiley Publishing, Inc.
- Kushner, D. (2013). The real story of stuxnet. *IEEE Spectrum*, 50(3), 48-53. doi:10.1109/MSPEC.2013.6471059. <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>.
- Ladley, J. (2012). *Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program*. Elsevier.
- Laing II, F. (2006). Multifactor authentication: What it means to you. (Cover story). *North Western Financial Review*, 191(17), 20.
- Langner, R. (2011). Stuxnet: dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3), 49-51. doi:10.1109/MSP.2011.67.
- Legal Information Institute. (n.d.). 31 U.S. Code § 5312 - Definitions and application. Retrieved August 22, 2021, from

- <https://www.law.cornell.edu/uscode/text/31/5312>
- Levanti, N. M. (2014). *Walking on air – The dangers of cloud computing*.  
<http://www.europeanpublicaffairs.eu/walking-on-air-the-dangers-of-cloud-computing/>
- Lew, J. J. (2014). Remarks of Secretary Jacob J. Lew. *Delivering Alpha Conference*. <http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx>.
- Lipner, S.B. (2015). The Birth and Death of the Orange Book. *IEEE Annals of the History of Computing* 37(2), 19-31. <https://www.muse.jhu.edu/article/584410>.
- Lockhardt, C. (2012). The human factor: Using behavioral science to counter insider threats. *MITRE*. <http://www.mitre.org/publications/project-stories/the-human-factor-using-behavioral-science-to-counter-insider-threats>
- Macwelch, T. (2015). EMP survival: 9 ways to prepare for an electro-magnetic pulse. *Outdoor Life*.  
<http://www.outdoorlife.com/photos/gallery/2015/05/emp-survival-9-ways-prepare-electro-magnetic-pulse>
- Mandal, S., Khan, D.A., & Jain, S. (2021). Cloud-based zero trust access control policy: An approach to support work-from-home driven by COVID-19 pandemic. *New Generation Computing*, 39, 599–622.  
<https://doi.org/10.1007/s00354-021-00130-6>
- Mandiant. (2023). *M-Trends 2023: Cybersecurity insights from the frontlines*.  
<https://www.mandiant.com>
- Mell, P., & Grance, T. (2011, September). *SP 800-145: The Definition of Cloud Computing*. Retrieved from National Institute of Standards and Technology:  
<https://csrc.nist.gov/publications/detail/sp/800-145/final>
- Merhout, J. W., & Havelka, D. (2008). Information technology auditing: A value-added IT governance partnership between IT Management and Audit. *Communications Of The Association For Information Systems*, 23,

463-482.

Mermod, A. (2011). Customer's perspectives and risk issues on e-banking in Turkey: Should we still be online? *Journal Of Internet Banking & Commerce*, 16(1), 1-15.

Merriam-Webster. (n.d.). *Technology*. Retrieved October 2020 from Merriam-Webster.com dictionary: <https://www.merriam-webster.com/dictionary/technology>

Microsoft. (2012). System center configuration manager (Version 2012 R2) [Software]. Retrieved August 5, 2014, from <http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2-configuration-manager/default.aspx?nv1if0=1>

Microsoft. (2023). What is cloud computing? <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/>

Mohanty, S., Pattnaik, P. K., & Mund, G. B. (2014). Framework for auditing in cloud computing environment. *Journal Of Theoretical & Applied Information Technology*, 65(1), 261-267.

National Credit Union Administration (NCUA). (2022, April 25). *About*. <https://www.ncua.gov/about>

National Institute of Standards and Technology (NIST). (2007). *Information security handbook: A guide for managers*. <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>

National Institute of Standards and Technology (NIST). (2009). *Guide to enterprise password management (draft)*. Special Publication 800-118 (SP 800-118, Draft). <http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf>

National Institute of Standards and Technology (NIST). (2009). NISTIR 7621: *Small business information security: The fundamentals*. <http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf>

National Institute of Standards and Technology (NIST). (2010). Special publication

- 800-37: *Guide for applying the risk management framework to federal information systems*. <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
- National Institute of Standards and Technology (NIST). (2012) SP 800-30 Rev. 1: *Guide for conducting risk assessments*.  
[http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800\\_30\\_r1.pdf](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf)
- National Institute of Standards and Technology (NIST). (2013). Special publication 800-53: *Security and privacy controls for federal information systems and organizations*. V5.0. doi:10.6028/NIST.SP.800-53r4. Retrieved August 5, 2014, from  
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- National Institute of Standards and Technology (NIST). (2014) *Framework for improving critical infrastructure cybersecurity*.  
<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>
- National Institutes of Standards and Technology (NIST). (2009, September 29). *Information technology security for small business* [Video file].  
<https://www.youtube.com/embed/ajwX-7jVLo0>
- Network World. (2012). Application whitelisting is a viable option when you can leverage software signing. *Business Insights: Essentials*.
- Newitz, A. (2013, September 16). *The bizarre evolution of the word “cyber”*. Gizmodo. Retrieved December 26, 2023, from <https://gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487>
- Nonnenmacher, T. (2001, August 14). History of the U.S. telegraph industry. Retrieved from EH.Net Encyclopedia: <http://eh.net/encyclopedia/history-of-the-u-s-telegraph-industry/>
- Office of the Comptroller of the Currency (OCC). (2019, July). *Corporate and risk governance*. <https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk->



- governance/index-corporate-and-risk-governance.html
- Office of the Comptroller of the Currency (OCC). (n.d.). 12 CFR Part 30: *Safety and Soundness Standards*. [http://ithandbook.ffiec.gov/media/21989/occ-12cfr30-safe\\_sound\\_standards.pdf](http://ithandbook.ffiec.gov/media/21989/occ-12cfr30-safe_sound_standards.pdf)
- Office of the Comptroller of the Currency (OCC). (n.d.). *About us*. <https://www.occ.treas.gov/about/index-about.html>
- Office of the Comptroller of the Currency (OCC). (n.d.). *Sound Practices to Strengthen Operational Resilience*. <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-144a.pdf>
- Office of the Federal Register. (2019, March 29). Coordinating national resilience to electromagnetic pulses. *Federal Register*. <https://www.federalregister.gov/documents/2019/03/29/2019-06325/coordinating-national-resilience-to-electromagnetic-pulses>
- Olhorst, F. (2015). 5 Free Tools for Compliance Management. <http://www.esecurityplanet.com/open-source-security/slideshows/five-free-tools-for-compliance-management.html>
- Orozco, A. (2012, September 3). Hacker hands Barto manufacturer \$190,000 loss. *Reading Eagle (PA)*.
- Palazzolo, J. (2012, December 3). Proceedings / highlights from the law blog. *Wall Street Journal - Eastern Edition*, p. B7.
- Pavlov, G. G., & Karakaneva, J. J. (2011). Information security management systems in organization. *Trakia Journal Of Sciences*, 9(4), 20-25.
- Payment Card Industry (PCI). (2016). Data security standard: Version 3.2. [https://www.pcisecuritystandards.org/document\\_library?category=pcidss&document=pci\\_dss#agreement](https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss#agreement)
- Pinder, T. (2012). Rethink cyber security. *ABA Banking Journal*, 104(10), 61.
- Piper, F. (2003). An introduction to cryptography. *Information Systems Control Journal*, 6, 1-8. <http://www.isaca.org/Journal/Past-Issues/2003/Volume-6/Documents/jpdf036-AnIntrotoCryptography.pdf>

- Praisia Technologies. (2014, September 27). Big data security analytics – 2nd generation SIEM. LinkedIn Pulse.  
<https://www.linkedin.com/pulse/20140927204245-327286699-big-data-security-analytics-2nd-generation-siem>
- Prakash, P. (2020). Forming an LLC in NJ: A step-by-step guide. *Nerdwallet*.  
<https://www.nerdwallet.com/article/small-business/llc-nj>
- Rapid7. (n.d.). *Essentia health reduces risk with nexpose and metasploit*.  
<http://www.rapid7.com/docs/essentia-health-reduces-risk.pdf>
- Ray, M. (2023). Chelsea Manning. In *Britannica*.  
<https://www.britannica.com/biography/Chelsea-Manning>
- Reynolds, G. W. (2011). *Ethics in information technology, 4th edition*.
- Roberts, C. (2019, October 8). *Study: Banks will replace 200,000 workers with robots by next decade*. Observer. <https://observer.com/2019/10/banks-robots-replace-tellers-wells-fargo-study/>
- Ross, R., Swanson, M., Katzke, S., Stoneburner, G., Greene, J. F., Williams, P., . . . Cussatt, D. (2010). National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 1: *Guide for applying the risk management framework to federal information systems: A security life cycle approach*. <http://dx.doi.org/10.6028/NIST.SP.800-37r1>
- Rouse, M. (2015, May 26). *Trojan horse* [definition]. Tech Target.  
<https://www.techtarget.com/searchsecurity/definition/Trojan-horse>
- Rupasri, M., Rajyalakshmi, P., Shanmugasund, V., & Sangeeta, V. (2012). A Study of Buffer Overflow Attacks. *International Journal of Engineering and Advanced Technology*, (4), 140.
- Ryan, D. (2016). FinCEN: Know your customer requirements. *Harvard Law School Forum on Corporate Governance and Financial Regulation*.  
<https://corpgov.law.harvard.edu/2016/02/07/fincen-know-your-customer-requirements/>
- Ryckman, P. (2012, June 14). Owners may not be covered when hackers wipe out a

- business bank account. *New York Times*, p. 11
- SANS Institute. (2013). Critical security controls for effective cyber defense. Retrieved August 5, 2014, from <https://www.sans.org/critical-security-controls/>
- Sarbanes-Oxley (SOX). (2002). Act of 2002, Pub. L. 107-204, 116 Stat. 745, codified as amended at 15 U.S.C. § 7241 & 18 U.S.C. § 1350. [http://ithandbook.ffiec.gov/media/20866/con-pl\\_107\\_204\\_116sta745-sarbanes\\_oxley.pdf](http://ithandbook.ffiec.gov/media/20866/con-pl_107_204_116sta745-sarbanes_oxley.pdf)
- Sausner, R. (2011). FFIEC to revisit online protection. *Bank Technology News*, 24(3), 1-11.
- Scarola, A. (2015, October). Security of Cloud Computing. <https://cloud-security.cloudcomputingoutlook.com/cxoinsights/security-of-cloud-computing-nid-132.html>
- Schneier, B. (2010, October 7). Stuxnet [Web log post]. <http://www.schneier.com/blog/archives/2010/10/stuxnet.html>
- Seltzer, L. (2013). Security and the ‘if it ain’t broke don’t fix it’ mentality. *Betanews*. <https://betanews.com/2013/06/28/security-and-the-if-it-aint-broke-dont-fix-it-mentality/>
- Sequel Data Systems Incorporated. (2015, September 30). How big data security analytics is transforming enterprise security. Sequel Data Systems Incorporated. <http://www.sequeldata.com/how-big-data-security-analytics-is-transforming-enterprise-security>
- Sokolow, A. (2011, August 15). Sun, surf, Internet: how to ensure safe online access during vacation. *dpa (Hamburg, Germany)*.
- Sood, A., & Enbody, R. (2011). The state of HTTP declarative security in online banking websites. *Computer Fraud & Security*, 2011(7), 11-16. doi:10.1016/S1361-3723(11)70073-2.
- Sophos. (2023, July 13). *The state of ransomware in financial services 2023*. Sophos. <https://news.sophos.com/en-us/2023/07/13/the-state-of->

- ransomware-in-financial-services-2023/
- Symantec. (2012). Symantec Survey Reveals Online File Sharing Poses Great Security Risks to SMBs. *TendersInfo News*.
- Talabis, M., & Martin, J. (2015). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Syngress.
- Taleghani, M., Sharifi, A., & Gilaninia, S. (2011). The role of key factors in e-banking for new enterprises (concepts & applications). *Interdisciplinary Journal of Contemporary Research In Business*, 3(3), 999-1006.
- Task Force on Home Banking Services Agreement, ABA Section of Business Law. (2006). Home Banking Services Agreement. *The Business Lawyer*, 611-640.
- Taylor, L. (2016). The rise of remote working and the “coffee-shop worker”. *Engadget*. <https://www.engadget.com/2016/09/19/the-rise-of-remote-working-and-the-coffee-shop-worker/>
- TechHQ. (2024, January 17). *Apple’s GenAI version of Siri rumored to land this year*. <https://techhq.com/2024/01/is-siri-ai-coming-in-2024/>
- Tenable Network Security. (n.d.). Bitbrains case study. <http://www.tenable.com/case-studies/bitbrains>
- Thales. (2023). *Data threat report - Financial services edition*. <https://cpl.thalesgroup.com/financial-services-data-threat-report>
- The President of the United States. (2013). Executive order 13636: Improving critical infrastructure cybersecurity. *U.S. Government Printing Office*. <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.
- Tipton, H. (n.d.). Access control principles and objectives: Types of information security controls. *Information Security Management Handbook*. Auerbach Publications and CRC Press, Boca Raton, FL.
- Townsend, K. (2022, July 11). *The history and evolution of zero trust*. SecurityWeek. <https://www.securityweek.com/history-and-evolution-zero-trust/>
- Two River Community Bank. (2016). The high cost and risk of using old computer

- technology. <https://www.tworiverbank.com/2016/05/19/high-cost-risk-using-old-computer-technology/>
- U.S. Code; Banks and banking; management; supervisory committee, 12 U.S.C. § 1761d. [http://ithandbook.ffiec.gov/media/20887/con-12usc1761\\_and\\_1761d\\_sup\\_commit.pdf](http://ithandbook.ffiec.gov/media/20887/con-12usc1761_and_1761d_sup_commit.pdf)
- U.S. Government Accountability Office (GAO). (2017, December). Electricity suppliers have taken actions to address electromagnetic risks, and additional research is ongoing (GAO-18-67). <https://www.gao.gov/assets/gao-18-67.pdf>
- U.S. v. Bradley Manning. (n.d.). In *Wikipedia*. Retrieved January 17, 2022, from [https://en.wikipedia.org/wiki/United\\_States\\_v.\\_Manning](https://en.wikipedia.org/wiki/United_States_v._Manning)
- Vahromovs, V. (2024, January 3). *Legacy systems in banking: the major barrier for digital transformation*. FinTech Futures. <https://www.fintechfutures.com/2021/11/legacy-systems-in-banking-the-major-barrier-for-digital-transformation/>
- Virginia Law. (2014). Breach of personal information notification. <https://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/>
- Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.
- Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. (n.d.). Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, 55(4), 345-362.
- Ware, V. Y. (2011). A new security blueprint. *Independent Banker*, 61(12), 60-62.
- White House. (2003). *The National Strategy to Secure Cyberspace*. <https://nsarchive.gwu.edu/sites/default/files/documents/2700096/Document-16.pdf>
- White, C. (2021, March 28). *Consumer Protection in the Fintech Era*. St. Louis Fed. <https://www.stlouisfed.org/on-the-economy/2021/march/consumer->

protection-fintech-era

Whittaker, S. (2007, May 12). *The Montreal Gazette*. Retrieved from Wayback Machine:

<https://web.archive.org/web/20160304090328/http://www.canada.com/montrealgazette/story.html?id=78fc94dd-c0b2-4ade-891d-98770bfae388&k=70777>

Zakrzewski, A., Tang, T., Appell, G., Fages, R., Hardie, A., Hildebrandt, N., . . .

Xavier, A. (2019, June 20). *Global wealth 2019: Reigniting radical growth*. Retrieved from Boston Consulting Group: [https://image-src.bcg.com/Images/BCG-Reigniting-Radical-Growth-June-2019\\_tcm9-222638.pdf](https://image-src.bcg.com/Images/BCG-Reigniting-Radical-Growth-June-2019_tcm9-222638.pdf)

Zetter, K. (2011, August 26). Researchers uncover RSA phishing attack, hiding in plain sight. *Wired*. <https://www.wired.com/2011/08/how-rsa-got-hacked/>