# Accenture PLC and Cybersecurity on a Global Scale

David A. Wagle

School of Business, Northcentral University TIM-8301: Principles of Cybersecurity

Dr. Bill Souza May 2, 2021

# Accenture PLC and Cybersecurity on a Global Scale Introduction

Accenture is a multinational professional services company with a primary focus on technology delivery and the enablement of innovation. Accenture’s headquarters are in Dublin, Ireland. Their current client list includes 75% of the “Global Fortune 500” including more than 90 of the “Fortune 100.” Accenture reported over $43B US in revenue in 2019. Accenture employs more than 500,000 people worldwide (Accenture PLC, [2019).](#_bookmark0) Accenture’s business model divides the company into five primary operating segments: Communications, Media & Technology, Health & Public Services, Products, and Resources. These operating segments function across the globe in over 120 countries (Wagle, [2020c).](#_bookmark21)

There are several obvious commonalities across the most important of Accenture’s clients. First is size and scale. Accenture currently is serving over 6,000 clients globally. But these are not small entities. Clients are other large scale organizations that can make investments in technology from $10s of millions up to multiple hundreds of millions per quarter. The Diamond Clients, in 2019, consisted of almost entirely Global Fortune 1000 companies. These included 91 Fortune Global 100 clients (Wagle, [2020a).](#_bookmark19)

Given size of engagements that Accenture seeks, clients are limited to large entities with extensive revenues and government entities with large budgets. The average reported revenues of Accenture’s publically traded clients exceeds $500M annually, and the vast majority exceed $1B. Clients are generally national or global in their own scope, though larger regional entities, particularly insurance and financial service providers, do make the client list. The five operational groups break down to 13 focused industry groups, and more than 40 industries. Accenture does not make the data at these levels of breakdown public (Wagle, [2020b).](#_bookmark20)

Accenture is well-regarded as a primary implementer of customer relationship management (CRM), enterprise resource planning (ERP), enterprise resource management (ERM), and similar enterprise scale systems. These systems are highly complex, and

require significant expertise to configure correctly (AboAbdo et al., [201](#_bookmark1)9). This is expertise that the client is unlikely to posses directly. Moreover, often the client will need to engage in cultural transformations to be successful. Such transformational needs often require a trusted partner for success (Kimpel, [2020).](#_bookmark10)

Demonstrated capability in cybersecurity is doubly important for a company such as Accenture. Not only are company secrets invaluable for addressing considerations such as contract bids and customer relationship management issues, they also often contain client information which is equally if not more sensitive, much like law firms (Ries & Plc, [2018),](#_bookmark15) consultancy companies have an ethical and contractual duty to protect their clients.

# Risk

Accenture faces the typical cybersecurity threats of any major corporation. The most common, and arguably the most dangerous risks faced by Accenture, as with most companies, are risks of human behavior. Employees falling for phishing attacks, installing unauthorized software, providing information over the phone, or otherwise falling for human engineering attacks remains a top vector for initiating attacks. This is especially true for human beings who are under time pressure, as most busy consultants generally are (Chowdhury et al., [2](#_bookmark6)019).

The to external threats that companies such as Accenture are most likely to see that are directed at Accenture or its employees directly are malware attacks, web-based attacks, web-application attacks, phishing, distributed denial of service, spam, botnets, data breaches, and information leakage (Kettani & Wainwright, [2019).](#_bookmark9) Additionally, top internal threats are insider data theft, and physical damage or loss.

In addition to these common attack types aimed at Accenture and its employees, due to the fact that Accenture’s client base includes most of the largest companies and governments in the world, significant cyber espionage aimed at the client base is also a real threat. Such attacks can be focused on obtaining client trade secrets (Levine & Seaman,

[2018),](#_bookmark12) disrupting client business ventures, or at furthering or creating geopolitical outcomes. This latter risk can be either as a stand-alone activity or part of a hybrid-threat model with non-cyber attacks as part of the strategy (Mareşi, [2020).](#_bookmark13)

Additionally, as Accenture works in the energy field, supply chain management arena, and in helping clients build complex products requiring complicated control systems, Accenture must be aware of attacks aimed specifically at these arenas. Each of these fields has seen a rise of sophisticated attacks aimed not at specific companies, but at the societal or global functions they provide. For example, attacks aimed specifically at disrupting the energy grid rather than harming a particular energy company (Ahmadian et al., [2018),](#_bookmark2) or attacks at control systems used across multiple companies (Busby et al., [2017).](#_bookmark4)

Risk identification for such a large and diverse organization is primarily about identifying what the common current risks facing companies in general are. Afterall, a global attack surface is quite likely to experience attacks that mirror the global averages to a large degree.

Additionally, the company must be aware of the foreign policy objectives of the major governmental clients of the company and the geopolitical climate and strategic actors in the regions where the company operates. For example, with operations in both the United States as well as numerous SouthEast Asian nations, including China, analysis of risk for Accenture must include awareness of all of foreign policy (Chapman, [2018;](#_bookmark5) Singh, [2020).](#_bookmark17)

Obvious harms from cybersecurity attacks against Accenture include the commonly seens harms of financial loss, harm to reputation, loss of productivity, loss of client trust, and others. But less obvious harms include those that would result from subversion of client interests, reputation, productivity, and trust. For an example of one famous case detailing the extent to which external parties can be harmed, lost laptops from employees and contractors cost the Department of Veteran Affairs tens of millions of dollars in notification and monitoring procedures, another $20 million in a class action lawsuit, and

additional costs (Nagesh, [2010).](#_bookmark14)

A more significant case of the magnitude of fallout that can be experienced from breaching Accenture, or from an insider threat within Accenture, can be seen in the cases of Edward Snowden and Wikileaks.

Snowden was an employee of Booz Allen Hamilton (an Accenture competitor) working on contract with the NSA. Snowden famously revealed numerous top-secret documents to the public outlining so-called warrantless-wiretapping programs being used in the USA domestically as part of the “war on terror” (Greenwald, [2013).](#_bookmark7)

WikiLeaks is an on-going international effort to publish “leaked,” data from governments and international companies provided by anonymous sources. Started in 2010 by Julian Assange, an Australian ex-pat , WikiLeaks holds as it’s mission the purpose of “throwing grit in the machine” (Zittrain & Suater, [2010).](#_bookmark22)

Given Accenture’s masive client base, the international interests in those clients, the competing nature of many of the clients, the governmental access that exists, and the sensative systems that Accenture works both on and with, the economic and social magnitude of the risk of cybersecurity failure for Accenture is difficult to overstate.

# Protecting Accenture from Cybersecurity Risks

Addressing the significant risks faced by Accenture from cybersecurity threats requires a robust and extensive response. The response must address “the Five Hard Problems” as defined by the National Security Agency. These problems are: scalability and composability; policy-governed secure collaboration; security-metrics-driven evaluation, design, development and deployment; resillient architectures; and, understanding and accounting for human behavior (Scala et al., [2019).](#_bookmark16)

These domains are defined by the NSA in response to the realization that security at scale generates unique problems of its own, some of which are currently unsolvable. As an example of the scalability and composability problem, consider the problem presented

by web applications at Accenture. Building reasonably secure web-services, understanding how to scan them for vulnerabilities, keep them patched, and so forth, is relatively well understood (Krohn, [2006).](#_bookmark11) However, the interaction of the thousands of internal

web-services within Accenture generates a network-effect that dramatically complicates the security question. A single web-service is easy to test for security. But when thousands of such services are able to interact with each other, the possible number of combinations scale exponentially. Testing each of these possible interaction chains requires traversing each possible path through the network graph for security. This is computationally impossible.

To address the “hard problems” then, Accenture must accept incomplete and imperfect solutions. But at a minimum, there must be a concerted effort to do the following: train and monitor employees and contractors continuously; protect against common external threats; maintain patching and system configuration compliance; automate scans for external and internal threats; build a robust response team for realized threats.

# Employee Training and Monitoring

Employees must be provided with engaging cybersecurity training on a near continuous basis. Annual one-time training is known to be only marginally effective. A much better strategy is to provide on-going training to reduce security risks (Hanna, [2020).](#_bookmark8) Additionally, automated tools must be developed that track employee’s behavior and employee tool compliance. Employee’s must not be allowed to install unauthorized software on their systems or access external storage systems (either physical devices or

network-based storage services) without a clear and documented business need. AI systems can be developed to look for behavior patterns that merit investigation, such as attempting to access unauthorized systems repeatedly, or other suspicious behaviors.

# Protect Against External Threats

External threats such as phishing attacks, malware, and so forth must be addressed. Employing common tools such as email scanners for suspicious links, using filtering proxies to block known blacklist sites, installing and updating anti-virus software, and other common practices must be implemented. External firewalls should include both

packet-filtering and proxy techniques to make incoming attacks more challenging. External systems must be routinely configured to prevent DNS leaks, and to ensure only required incoming connections on secure protocols are allowed. Internal systems must require

two-factor authentication for any external inbound connections. Critical internal business systems must require two-factor authentication at all times. Systems should be configured with the principle of least privilege.

Intrusion detection tools, such as Snort, must be implemented, configured, and monitored constantly. Systems must maintain robust logs and the logs must be analyzed for attempted exploits.

# Patching and Commpliance

All systems must be covered by a patching process that ensures the systems are regularly patched and kept up to date. Security patch releases for all vendors must be consistently monitored and patches above particular thresholds must be applied immediately whenever possible.

Security bullitens must be monitored for unpatched vulnerabilities. When such vulnerabilities are disclosed, Accenture must take steps to remedidate any impact from such vulnerabilities until an official patch, fix, or work-around is released.

System configuration and control standards must be established. Automated compliance scanning tools must be implemented to ensure that such configurations are maintained. Configuration changes must be logged and authorization records maintained.

# Scanning

System scanning and automated network and system testing must be robust and omnipresent. Where feasable, redundant scanning systems should be employed to ensure no “misses” in scans. Scans must address all aspects of system configuration, utilization, performance, and compliance. Scans must include all network interfaces, both internal and external. Additionally, any connections to or from vendors must be heavily scanned for intrusion events.

# Response Team

Accenture must have a robust, international, 24x7 response team. This team must have the access and knowledge to not merely identify, stop, and remediate cybersecurity threats to Accenture, but must also have access to senior leadership in order to address client impacts. This team must include experts in the field of law, communications, disaster response and recovery, as well as all reasonable cybersecurity domains.

This team must have access to tools and information necessary to address problems from as simple as a lost laptop to as complex as a major data breach of a global client.

This team must be multinational in scope, and be able to operate and communicate within every region where Accenture operates.

# Estimating Costs

Given Accenture’s size and scale, this will be a costly effort. At over 500,000 employees, staffing the response team just for employee-related security events such as lost laptops or accidentally mailing client data to the wrong client will require a large, global staff of highly trained specialist. Luckily for Accenture, as a highly prized employeer, finding and staffing such people is part of their business model.

Given the massive scale of this undertaking, the easiest way to anticipate budget is to simply look at industry figures. The average spend on IT security is 15% of the IT

budget, with almost a fourth of organizations spending more than 20%. Further, the size of the organization does not seem to matter much in these calculations (Violino, [20](#_bookmark18)19). It is not clear from Accenture’s annual report what their internal IT budget is. However, Accenture owns very little real property, leasing most of their office space. Further, their non-sales, non-consulting staff are relatively few with the excpetion of the internal IT department.

For these reasons, it is reasonable to assume that 75% of the “General and Administrative” costs category would be the internal IT budget. Thus, the assumed IT budget based on the 2020 annual report would be $2.1B (Accenture PLC, [2020).](#_bookmark3) Given Accenture’s high risk profile, it is reasonable to presume that Accenture would be on the high side of the industry average. Thus, cybersecurity budget for fiscal 2021 should be 20% of $2.1B, or $420M USD.

# References

AboAbdo, S., Aldhoiena, A., & Al-Amrib, H. (2019). Implementing enterprise resource planning erp system in a large construction company in ksa. *Procedia Computer* *Science*, *164*, 463–470. <https://doi.org/10.1016/j.procs.2019.12.207>

Accenture PLC. (2019). Leading with value: Accenture annual report 2019. Accenture PLC. (2020, August). Accenture 2020 annual report.

Ahmadian, S., Malki, H., & Han, Z. (2018). Cyber attacks on smart energy grids using generative adverserial networks. *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Signal and Information Processing (GlobalSIP), 2018 IEEE Global Conference on*, 942–946. <https://doi.org/10.1109/GlobalSIP.2018.8646424>

Busby, J. S., Green, B., & Hutchison, D. (2017). Analysis of affordance, time, and adaptation in the assessment of industrial control system cybersecurity risk: Analysis of affordance, time, and adaptation. *Risk Analysis*, *37* (7), 1298–1314. <https://doi.org/10.1111/risa.12681>

Chapman, B. (2018). U.s.–china economic and security review commission: Emerging factor in western pacific strategic policy analysis. *Geopolitics, History, and* *International Relations*, *10* (1), 7. <https://doi.org/10.22381/GHIR10120181>

Chowdhury, N. H., Adam, M. T. P., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behaviour & Information* *Technology*, *38* (12), 1290–1308. <https://doi.org/10.1080/0144929X.2019.1583769>

Greenwald, G. (2013, June 11). *Edward snowden: The whistleblower behind the nsa surveillance revelations*. the Guardian. Retrieved May 2, 2021, from [http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-](http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance) [whistleblower-surveillance](http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance)

Hanna, M. M. (2020). *Exploring cybersecurity awareness and training strategies to protect information systems and data* (*12-B*). ProQuest Information & Learning. Retrieved

May 2, 2021, from [http://proxy1.ncu.edu/login?url=https:](http://proxy1.ncu.edu/login?url=https)

//search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2020-51431- 041&site=eds-live

Kettani, H., & Wainwright, P. (2019, March). On the top threats to cyber systems, In *2019 ieee 2nd international conference on information and computer technologies (icict)*. 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT), Kahului, HI, USA, IEEE. <https://doi.org/10.1109/INFOCT.2019.8711324>

Kimpel, J. (2020). Measuring the impact of culture on critical success factors for global information system implementations. *Journal of Behavioral & Applied Management*, *20* (1), 36–50. <https://doi.org/10.21818/jbam.19.20.1.3>

Krohn, M. ( N. (2006). Building fast and secure web services with okws. Retrieved May 2, 2021, from [http://proxy1.ncu.edu/login?url=https:](http://proxy1.ncu.edu/login?url=https)

//search.ebscohost.com/login.aspx?direct=true&db=edsndl&AN=edsndl.oai.union. ndltd.org.MIT.oai.dspace.mit.edu.1721.1.34364&site=eds-live

Levine, D. S., & Seaman, C. B. (2018). The dtsa at one: An empirical study of the first year of litigation under the defend trade secrets act. *Wake Forest Law Review*, *53* (1), 105–156. Retrieved May 2, 2021, from

http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/login.aspx?direct= true&db=bth&AN=131004946&site=eds-live

Mareşi, C. N. (2020). Offensive cyber operations, an essential capability of hybrid threats.

*Strategic Impact*, *77* (4), 137–151. Retrieved May 2, 2021, from http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/login.aspx?direct= true&db=tsh&AN=149357557&site=eds-live

Nagesh, G. (2010, May 13). *Va loses another laptop with veterans’ personal data, prompting inquiry*. TheHill. Retrieved May 2, 2021, from [https://thehill.com/policy/technology/97817-va-loses-another-laptop-with-](https://thehill.com/policy/technology/97817-va-loses-another-laptop-with-veterans-personal-information) [veterans-personal-information](https://thehill.com/policy/technology/97817-va-loses-another-laptop-with-veterans-personal-information)

Ries, D. G., & Plc, C. H. (2018). Safeguarding client data: Attorneys’ legal and ethical duties. *Trusts & Estates*, 15.

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39* (10), 2119–2126. <https://doi.org/10.1111/risa.13309>

\_eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/risa.13309

Singh, D. (2020). American foreign policy and southeast asia. *Southeast Asian Affairs*, 57–75. Retrieved May 2, 2021, from http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/login.aspx?direct= true&db=a9h&AN=143747043&site=eds-live

Violino, B. (2019, August 20). *How much should you spend on security?* CSO Online. Retrieved May 2, 2021, from [https://www.csoonline.com/article/3432138/how-](https://www.csoonline.com/article/3432138/how-much-should-you-spend-on-security.html) [much-should-you-spend-on-security.html](https://www.csoonline.com/article/3432138/how-much-should-you-spend-on-security.html)

Wagle, D. (2020a). Client analysis: Accenture plc. *Unpublished*.

Wagle, D. (2020b). An evaluation of the financial status of accenture plc. *Unpublished*. Wagle, D. (2020c). Swot analysis: Accenture plc. *Unpublished*.

Zittrain, J., & Suater, M. (2010). Everything you need to know about wikileaks | mit technology review [magazine]. *MIT Technology Review*. Retrieved May 2, 2021, from [https://www.technologyreview.com/2010/12/09/120156/everything-you-need-to-](https://www.technologyreview.com/2010/12/09/120156/everything-you-need-to-know-about-wikileaks/) [know-about-wikileaks/](https://www.technologyreview.com/2010/12/09/120156/everything-you-need-to-know-about-wikileaks/)