# Accenture and Cybersecurity

David A. Wagle

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

Dr. Bill Souza date

# Accenture and Cybersecurity Mitigation Through Controls

Accenture, PLC. (https://accenture.com), is a multinational consulting company. In 2020 Accenture reported $44.33B US in revenues and employed nearly 550,000 people (Accenture PLC, [2020).](#_bookmark4) Accenture is the largest information technology consulting firm in the world by sheer number of employees and number of nations in which operates. It is second to Tata Consultancy Services in terms of total revenues. Accenture operates in more than 120 countries world-wide and its client list includes nearly 80% of the Global Fortune 500, more than 90 of the Fortune 100, and many G20 Governments and Government Agencies (Accenture PLC, [2020;](#_bookmark4) Wagle, [2020).](#_bookmark20)

In order to ensure the security of both client data and Accenture’s own internal data, Accenture includes numerous cybersecurity controls. Accenture is fully compliant with ISO/IEC 27001:2013, the international standard for information security (Accenture, [2021c)](#_bookmark2) as well as the European Union’s General Data Protection Regulation (GDPR).

ISO/IEC 24001:2013 includes 114 controls that are divided into 14 control sets as part of Annex A. Of these mitigating controls, four stand out as being of utmost importance for a company of Accenture’s size and scope. These are A.8 Asset Management, A.9 Access Control, A.7 Human Resource Security, and A.6 Organization of Information Security. This is not to say that the remaining areas are not highly important. Rather these four deserve special consideration simply because of the complexities involved when dealing with a corporation with the size and scope of Accenture.

# Asset Management

With more than half a billion employees alone, the number of laptops, cell phones, tablets and other personal devices Accenture must manage is staggering. Along with these personal devices, Accenture has an enormous corporate infrastructure. Accenture is 100% cloud-based in terms of their corporate functions, but they still maintain some assets in

datacenters for research and client support purposes (“Accenture Cloud First Launches with $3 Billion Investment to Accelerate Clients’ Move to Cloud and Digital Transformation”, [2020;](#_bookmark3) Accenture PLC, [2020).](#_bookmark4)

A fundamental principal of cybersecurtiy is that a company “cannot defend what they do not know they have” (Center for Internet Security, [2021).](#_bookmark7) Asset management includes not merely awareness of the devices, but of locations, versions, licenses and lifecycles. Large-scale asset management is a complex process that requires advanced techniques to perform well (Halima Ibrahim Kure & Shareeful Islam, [2019).](#_bookmark9) To this end Accenture uses a complex system of in-house developed tools, commercial products, and advanced AI techniques to continually monitor and poll their assets for cybersecurity purposes.

This is one of the more expensive areas of cybersecurity management for Accenture. However, the cost is justified based purely on the importance of being able to ensure access points to Accenture’s network, data, and client resources are known and properly monitored. Deployment of these tools is relatively straightforward as they are “baked” into the standard system images that are used for physical, virtual, and cloud devices. Once built into the deployment images, these tools are updated and configured automatically using remote management tool suites.

# Access Control

Accenture follows the principal of least privilege to ensure that data, systems, and tools are only accessible to those who have a need to access them, and that the users’ associated level of access grants them only the privileges they need to perform their role (Center for Internet Security, [2021;](#_bookmark7) Jillepalli et al., [2017).](#_bookmark14)

This control is highly important for an organization that is largely cloud-based and spans the entire globe. It is unrealistic to think that half-a-million employees would all exercise proper judgement at all times with regard to application usage, data usage, and

client confidentiality. Therefore, using access controls to ensure that only proper access happens is essential.

This is a relatively low-cost solution in practice as well. Accenture uses a single sign on system. This technology means that a user’s access rights are stored as part of the access credentialing system. Routine audits and manager and director level access request approvals creates a multi-level set of checks to ensure proper access is maintained.

Research has shown that collective, social, work-group level focus on security enhances overall security so there is some evidence that this type of structure is effective (Chul Woo Yoo et al., [2020).](#_bookmark8)

# A.7 Human Resource Security

Human Resource Security is easily the most costly and difficult to manage mitigating cybersecurity control. Accenture’s process starts with pre-employment background security checks as part of the hiring process. Once hired, employees are required to attend literally dozens of cybersecurity training courses spread over the course of each year. This on-going training touches on every aspect of security, from how to configure home wifi networks to legal and regulatory demands. Passing in-depth quizes on these topics is a requirement for all employees, and failure to maintain training can be grounds for termination.

Additionally, employees behavior is monitored in a variety of ways. For example, fack phishing emails are regularly sent to employees. Employees who fail to spot fake phishing attempts and react correctly will have their mailbox and accesses restricted for a full year, their managers will be notified of their compliance failure, and they will be required to attend signficiant remedial training.

The cost-benefit analysis of cybersecurity training is, however, cost-effective as so many cybersecurity incidents start from employees failing to social engineering attacks (Zhang et al., [2021).](#_bookmark21)

# A.18 Organization of Information Security

Lastly, there is the organization of information security. The goal of Annex A.6 is “to establish a management framework to initiate and control the implementation and operation of information security wtihin the organization” (IT Governance, [2021).](#_bookmark12) For an organization the size of Accenture, this is incredibly important. It is entirely unreasonable to presume that disparate groups could coordinate the implementation and management of cybersecurity compliance and mitigation measures globally. Thus, a centralized body focused on this effort is needed.

Interestingly, this internal central organization, while complex to establish and operate, is actually very cost efficient. This is due to the fact that Accenture uses this internal team to learn and develop client consulting offerings which are revenue generating. Because cybersecurity is an important client offering, Accenture is thus able to leverage this team’s internal activities against external clients.

# Mitigation, Continuity, and Disasters

The Colonial Pipeline shutdown of May, 2021, demonstrates the economic damage that can result from unmitigated cyber attacks. The shutdown was attributed to the impact of ransomware being successfully injected into the company’s IT systems (Sanger et al., [2021).](#_bookmark17) These types of attacks are typically the result of either successful human social engineering attempts or attacks on web-presence weaknesses (Sultan et al., [2018).](#_bookmark18)

Social engineering attacks are among the most successful of attacks for a variety of reasons and are growing in sophistication regularly (Krombholz et al., [2015).](#_bookmark15) Given the sheer number of employees of Accenture, it presents the largest opportunity for mitigation. This is not unique to Accenture. Social engineering is far less studied than other attack vectors, and researchers know less about why and how some social engineering attacks work and others fail. For example, what behaviors ranging from “passive, non-volitional non-compliance” to “volitional (but not malicious) non-compliance” are most useful for

social engineering exploiters (Dalal et al., [2021)?](#_bookmark10)

As was noted previously, Accenture’s focus on training and monitoring compliance against social engineering attacks such as phishing attacks is an important, as well as expensive, component of their overall cybersecurity framework. However, prevention is not the same as mitigation and ensuring of business continuity. Additional steps are necessary.

The first step to mitigating against social engineering attacks is the discipline of testing the effectiveness of training and placing those who fail the training under heavy restrictions. While it is indubitably expensive and time consuming for Accenture to continually test employees for their ability to avoid social engineering attacks, it pays off by allowing Accenture to reliably identify employees who don’t take social engineering attacks seriously. These employees have their access rights restricted and are subject to remedial training and heavier managerial oversight.

The second step to mitigating against social engineering attacks lays with the 100% cloud-based architecture that Accenture employs. Accenture can identify data and applications as either requiring multi-times and hour backup, hourly backup, multi-times a day backup, daily backup, or weekly backup. Cloud based solutions allows easy snapshots of critical data. If data is lost due to ransomware attacks or some other attack, then rolling back to a point where the data was not inaccessible is fairly easy to do (Amazon AWS, [2021).](#_bookmark5) By using a global cloud architecture with multiple, frequently tested, independent restoration paths, Accenture can guarantee a high degree of business continuity and disaster recovery from attacks similar to ransomware social engineering attacks.

Cloud based digital asset management also allows for high degree of flexibility and protection. Mobile assets can be tracked automatically with geolocation technologies, and users who travel to regions where threat levels are high can have their access restricted using geofencing (SyndiGate Media, [2020).](#_bookmark19)

Cloud-based access control models allow the easy layering of multiple access models ontop of one another. Role-based access controls can have context-based access control

models and attribute-based access controls models sitting on top of them.

Solid cloud-based architecture featuring frequently audited, role-based, least privilege access control also helps with mitigation. Access control mechanism preserve the so-called CIA triangle (confidentiality, availability, and integrity) from external attacks (Malik et al., [2020).](#_bookmark16)

Because access is limited to a strictly role-based privilege, no single account has the access necessary to truly disrupt any segment of Accenture business. Developers don’t have write access to datastores, for example. And those who create data are only given

write-access to the data rows they need to write data to based on their role. Further, access control can serve not just preventative functions, but can be used to detect, correct, and recovery from unwanted events as well (Malik et al., [2020)](#_bookmark16).

As an example of context-aware access controls, in association with asset control systems, a user can have their access limited or removed if their mobile device is not located where the user is supposed to be (Jih et al., [n.d.).](#_bookmark13) This simply control provides significant protections against lost devices or devices that are hijacked via remote connections. But it also offers client protection features.

Attribute-based Access Controls systems can serve as a secondary role-based model that is applied with greater granularity. For example, a consultant with multiple clients may hold multiple roles. By comparing the consultant’s primary role with the client data and the data objects for which access is being requested, differing levels of permission can be provided on a data-object by data-object basis (Hu et al., [2015).](#_bookmark11) This fine-grained control means that attackers have very little hope of gaining wide-spread access to critical data.

Governance is another key part of the mitigation, continuity, disaster recovery process. Accenture has a 24x7 organization known as ASOC, the Accenture Security Operations Center (Accenture, [2021b).](#_bookmark0) This group has a broad focus to protect the security and integrity of Accenture’s assets, from physical buildings and people to technology assets

to data and products. All of Accenture’s security training starts and ends with a simple commandment: if there is a security event, the first order of business is to call ASOC.

This simply step can be remarkably effective in mitigating damage of an on-going attack. ASOC has the power, for example, to stop all data read-and-write-jobs to client databases based on the enterprise ID of the person calling them. They also have connections to investigatory and legal bodies in every country in which Accenture operations. This allows them to take immediate steps to engage legal entities to help in protecting potential damage to client’s data or services as well.

ASOC also deploys agents to all devices identified through asset management to proactively protect against data loss (Accenture, [2021a).](#_bookmark1) These agents monitor for behaviors that are identified as risky, and flags and blocks such transfers in real-time. This strongly mitigates against data loss from successful cyberattacks, and helps ensure business continuity, thus preventing the need for disaster recovery.

With respect to disaster recovery, as has been noted, Accenture is 100% cloud-based for all business services. Every service is required to have a tested and verified disaster recovery plan, and Accenture uses multiple cloud providers to ensure that even major regional disasters that take out multiple provider datacenters allow for easy recovery of operations. As each enterprise tool is built and managed as it’s own entity, Accenture has a disaster recovery model that is demonstrably sustainable and performant because of their cloud architecture (Andrade et al., [2019).](#_bookmark6)

# References

Accenture. (2021a). *Data loss prevention*. Retrieved May 23, 2021, from <https://www.accenture.com/us-en/case-studies/technology/data-loss-prevention>

Accenture. (2021b). *Empowering our people to speak up*. Retrieved May 23, 2021, from <https://www.accenture.com/us-en/about/company/raise-concerns>

Accenture. (2021c). *Information security client data protection*. Retrieved May 22, 2021, from [https://www.accenture.com/us-en/case-studies/about/keeping-accenture-](https://www.accenture.com/us-en/case-studies/about/keeping-accenture-client-data-protected) [client-data-protected](https://www.accenture.com/us-en/case-studies/about/keeping-accenture-client-data-protected)

*Accenture cloud first launches with $3 billion investment to accelerate clients’ move to cloud and digital transformation*. (2020, September 17). Retrieved September 26, 2020, from [https://www.businesswire.com/news/home/20200917005256/en/Accenture-](https://www.businesswire.com/news/home/20200917005256/en/Accenture-Cloud-First-Launches-with-3-Billion-Investment-to-Accelerate-Clients’-Move-to-Cloud-and-Digital-Transformation) [Cloud-First-Launches-with-3-Billion-Investment-to-Accelerate-Clients%E2%80%99-](https://www.businesswire.com/news/home/20200917005256/en/Accenture-Cloud-First-Launches-with-3-Billion-Investment-to-Accelerate-Clients’-Move-to-Cloud-and-Digital-Transformation) [Move-to-Cloud-and-Digital-Transformation](https://www.businesswire.com/news/home/20200917005256/en/Accenture-Cloud-First-Launches-with-3-Billion-Investment-to-Accelerate-Clients’-Move-to-Cloud-and-Digital-Transformation)

Accenture PLC. (2020, August). Accenture 2020 annual report.

Amazon AWS. (2021). *Amazon ebs fast snapshot restore - amazon elastic compute cloud*.

Retrieved May 23, 2021, from [https:](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-fast-snapshot-restore.html)

[//docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-fast-snapshot-restore.html](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-fast-snapshot-restore.html) Andrade, E., Link to external site, t. link will open in a new window, & Nogueira, B.

(2019). Performability evaluation of a cloud-based disaster recovery solution for it environments. *Journal of Grid Computing*, *17* (3), 603–621. h[ttps://doi.org/http://dx.doi.org.proxy1.ncu.edu/10.1007/s10723-](http://dx.doi.org.proxy1.ncu.edu/10.1007/s10723-018-9446-2)018-9446-2

Center for Internet Security. (2021). *Center for internet security cis controls v.8*. Retrieved May 22, 2021, from <https://learn.cisecurity.org/control-download>

Chul Woo Yoo, Jahyun Goo, & Rao, H. R. (2020). Is cybersecurity a team sport? a multilevel examination of workgroup information security effectiveness. *MIS Quarterly*, *44* (2), 907–931. <https://doi.org/10.25300/MISQ/2020/15477>

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: Abundant opportunities for research at the interface. *Journal of Business and Psychology*. <https://doi.org/10.1007/s10869-021-09732-9>

Halima Ibrahim Kure, & Shareeful Islam. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical* *Systems*. <https://doi.org/10.1049/iet-cps.2018.5079>

Hu, V. C., Kuhn, D. R., Ferraiolo, D. F., & Voas, J. (2015). Attribute-based access control.

*Computer*, *48* (2), 85–88. <https://doi.org/10.1109/MC.2015.33>

IT Governance. (2021). *Iso 27001*. Retrieved May 22, 2021, from <https://itgovernance.co.uk/iso27001>

Jih, W.-r., Cheng, S.-y., Hsu, J. Y.-j., & Tsai, T.-M. (n.d.). Context-aware access control in pervasive healthcare, 8.

Jillepalli, A. A., Leon, D. C. de, Steiner, S., Sheldon, F. T., & Haney, M. A. (2017).

Hardening the client-side: A guide to enterprise-level hardening of web browsers. *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing*, 687–692. <https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.120>

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. <https://doi.org/10.1016/j.jisa.2014.09.005>

Malik, A. K., Emmanuel, N., Zafar, S., Khattak, H. A., Raza, B., Khan, S.,

Al-Bayatti, A. H., Alassafi, M. O., Alfakeeh, A. S., & Alqarni, M. A. (2020). From conventional to state-of-the-art iot access control models. *Electronics*, *9* (10), 1693. <https://doi.org/10.3390/electronics9101693>

Sanger, D. E., Krauss, C., & Perlroth, N. (2021). Cyberattack forces a shutdown of a top

u.s. pipeline [newspaper]. *The New York Times: U.S.* Retrieved May 22, 2021, from

[https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-](https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html) [pipeline.html](https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html)

Sultan, H., Khalique, A., Tanweer, S., & Shah, I. A. (2018). A survey on ransomeware: Evolution, growth, and impact. *International Journal of Advanced Research in Computer Science*, *9* (2), 802–810. h[ttps://doi.org/http://dx.doi.org.proxy1.ncu.edu/10.26483/ijarcs.v9i2.5858](http://dx.doi.org.proxy1.ncu.edu/10.26483/ijarcs.v9i2.5858)

SyndiGate Media. (2020). 10 ways asset intelligence improves cybersecurity resiliency and persistence. *Legal Monitor Worldwide*. Retrieved May 23, 2021, from http://proxy1.ncu.edu/login?url=https://search.ebscohost.com/login.aspx?direct= true&db=edsinc&AN=edsinc.A612557347&site=eds-live

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

Zhang, Z., He, W., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: A cost–benefit analysis framework. *Industrial Management & Data Systems*, *121* (3), 613–636. <https://doi.org/10.1108/IMDS-08-2020-0462>