White Paper

# Avanade's Approach to Client Data Protection

avanade

## The Threat Landscape

Businesses today face many risks and emerging threats to their IT systems and data. To achieve sustainable success in a global environment, they must secure and monitor their platforms, applications and deployed technology for cybersecurity attacks. The 2016 Microsoft Security Intelligence Report[1] shows an active global threat landscape of cyberattacks, as detected by the Microsoft Azure Security Center, broken down by country of origin (*see map below*).

In addition, according to the 2017 Verizon Data Breach Report,[2] organizations in the financial services (24%) and healthcare (15%) industries face the highest risk of data breaches, followed by those in the public sector (12%).

Avanade is ready to assist these organizations with their risk management and help protect their IT systems and data. Avanade's Client Data Protection (CDP) program meets or exceeds the data protection protocols requirements requested by our clients. This whitepaper details the importance of data protection, along with Avanade's guiding principles and approach to data protection. It also provides an overview of the Avanade CDP program and controls. The information in this document will help you understand how we work to protect our clients' data before and during client service delivery.


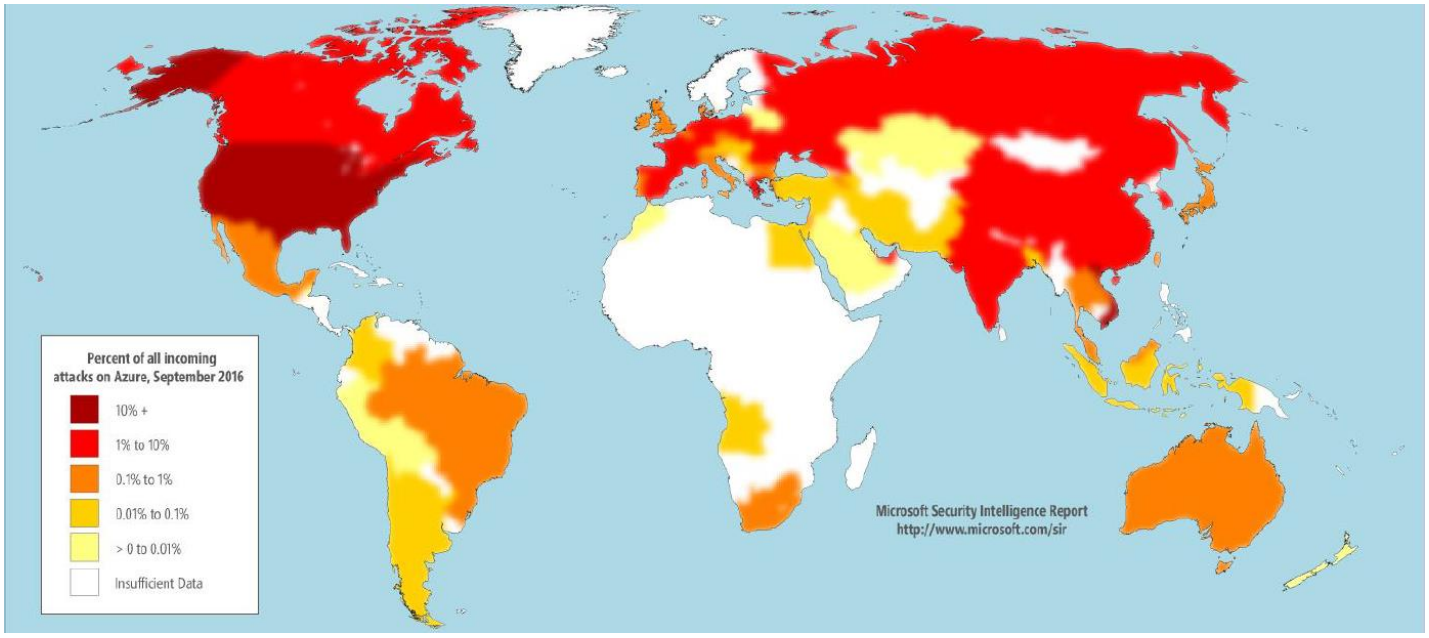


*Figure 1 Microsoft Security Intelligence Report Volume 21 - Incoming attacks detected by Azure Security Center in September 2016 by country/region of origin*

## Guiding Principles

**Responsibility**
Protecting our clients' data is a shared responsibility between Avanade and our clients. Safeguarding our clients' data is one of the most fundamental and important responsibilities we have at Avanade. Protecting that data is essential to maintaining client trust, and that trust is the cornerstone of every client relationship. Our CDP program leverages this shared responsibility by collaborating with our clients on the risk assessment and proactively working with them to leverage the security controls put in place in the CDP plan to protect our clients' data during all service delivery.

**Vulnerability**
It is crucial to address information security risk and mitigation after all client information assets, which are part of the service delivery, are inventoried and the asset valuation is determined. Asset valuation determines which security controls should be put in place to mitigate client risk and ensure that the cost-benefit ratio is not exceeded.

**Prevention**
Avanade's CDP program focuses on preventing security and data breaches to protect the business and personal data of our clients and their customers. We do not rely on insurance or blame. The Avanade CDP program is implemented for every client service delivery engagement.

**Clarity**
Clear policies and procedures are established to guide the Avanade CDP Program and provide for a consistent implementation across client engagements. Client CDP plans are monitored by the Avanade CDP team as well as the client service delivery team to ensure that clients' information security requirements are met.

# Avanade's Multi-Disciplinary Approach to Security

**Client Data Protection**
Avanade's CDP program governs the stewardship of client information entrusted to Avanade. The responsible service delivery team implements and monitors CDP plan execution, and all service delivery consultants authorized to work on the client service delivery engagement must follow that plan.

**Risk Management**
We understand our clients' business objectives, information security requirements and business risks well before the service delivery. The security controls utilized in Avanade's CDP program are designed to mitigate the client's risk to acceptable levels. The Avanade CDP program institutes continual monitoring and assessment of information security risk for our clients through risk assessments and deep dive audits to validate the effectiveness of security controls.

**Technology**
The Avanade CDP program team monitors and protects Avanade's overall technology environment used for service delivery to meet our clients' business and information security objectives. The CDP plan is continuously evaluated and monitored to assess how well it addresses information security risks within the technology environment of the service delivery engagement.

**Awareness and Training**
Ongoing awareness communications campaigns and mandatory data protection training are provided on a regular basis to all Avanade stakeholders. Avanade mandates annual compliance and information security training for all Avanade employees to ensure that protecting our clients' data is always a priority.

**Incident Response**
Incident response management is governed by Avanade's global security policies on Crisis Management, the Avanade Asset and Data Security Incident Response Reporting Standard and Avanade's global IT Security Policy. Response and remediation efforts are handled through our Global Delivery Network (GDN) centers and coordinated through the Avanade Asset Protection (AAP) program. Note that the CDP plan requires notification to AAP for any incident related to people or data. The AAP team mission is to protect our critical assets, and that includes our client services, offerings and Avanade employees. The AAP team vision is to protect our employees and business worldwide and provide instant response to questions or concerns regarding our employees, hardware and facilities. The AAP team helps plan remediating events and coordinates necessary corrective actions.

# CDP Program – Key Components

The Avanade CDP program is an industry-leading program, committed to long-term client relationships that are built on trust and inspire clients to put Avanade at the heart of their business. Every new client opportunity gives us more to protect and keeps us focused on demonstrating our stewardship of client information as if it were Avanade's own. Each of our clients brings unique security requirements, and we are committed to protecting our clients' data and systems across all client service delivery engagements.

CDP program key elements are:

**Accountability**
Senior level responsibility is assigned to an Avanade executive for data protection and mandatory program adoption for all engagements. Avanade assigns qualified CDP Executives (director level or above) for a client service delivery engagement. The CDP Executive is required to affirm plan completeness and implementation. An assessment is completed by the CDP Executive every three months, and an audit is done every six months. The assessment and audits are further covered in detail below. If the CDP Executive leaves the role, they are required to include their CDP responsibilities in the knowledge transition plan and notify the CDP team of their replacement. In addition, accountability for the security controls is required by ISO 27001 standards to which Avanade is aligned.

**Training and Awareness**
All Avanade employees are required to complete annual compliance and security training. Furthermore, the Avanade CDP plan implements mandatory security training for Avanade delivery teams. Based on the risk assessment score, additional training may be instituted. For example, all Health Insurance Portability Accountability Act (HIPAA) engagements and their CDP plans are automatically designated with a high-risk score, and additional HIPAA controls are implemented. This leads to the assignment of CDP HIPAA awareness training by roles, such as solution architects, benefits design and planning, as well as HIPAA training for delivery consultants who may be required to access Protected Health Information (PHI), and training on the HIPAA Business Associate Agreement (BAA). Note that these mitigation efforts for high-risk client engagements are not limited to HIPAA projects.

**Foundational Controls**
The Avanade CDP program includes required controls for storing, accessing, handling, transmitting and hosting client data. These security controls are included in every CDP plan assigned to the individual client service delivery engagement.

**Service Specific Controls**
The Avanade CDP plan includes controls tied to risks inherent in specific types of work and industries/ The CDP plan also includes controls that are necessary to meet our clients' specific information security requirements.

**Technology**
Technology support, including hard drive and USB encryption, workstation configuration scanning, web filtering and data loss prevention, are part of every CDP plan implemented for Avanade's clients.

**Subject Matter Expertise**
The CDP team provides tools, processes and subject matter specialist support to the project teams. It also provides guidance from the Avanade Connected Methods (ACM) delivery methodologies to help ensure consistency and quality to every solution and client service delivery. In addition, the Avanade Office of the Chief Information Security Officer (CISO) provides subject matter expertise for the CDP program.

# CDP Program – Preliminary Risk Assessment and Mitigation Plan

The Avanade CDP Program provides protection for clients' confidential data. The Avanade CDP program is a two-part program consisting of a risk assessment to determine where a client's risk lays in relation to the project, and based on the risk assessment score, a mitigation phase that uses a CDP plan comprised of up to twenty-nine security control categories operated by the client service delivery team. When designing the individual CDP plan for clients, various inputs are considered, such as data type and volume, scope of services, as well as contractual requirements. With the inputs gathered, the CDP team works with the service delivery team to (i) assess risk, (ii) identify gaps and develop action plans, (iii) implement program and close gaps, and (iv) monitor compliance and reassess:

**Assess Risk**
The CDP Risk Assessment (RA), required by Avanade Data Management Policy, is used to assess client risk before and during service delivery on all work orders with following engagement types. The client team is accountable for the RA being completed.

The RA measures where client's risk lays in relation to the project and what type of protection effort Avanade needs to take. Upon completion of the RA a low, medium or high-risk score is produced that determines the type of CDP plan required. RA scores also help estimating how many hours to dedicate for CDP. CDP Risk Assessments apply to all direct work at Avanade with the following Engagement Types. Staff augmentation WOs require a Risk Assessment (and must meet all criteria and get approval from the CDP HD). The risk analysis is utilized to understand data and operational risk to determine appropriate control requirements and oversight.

**Identify Gaps and Develop Action Plans**
Gap Analysis is conducted to identify control gaps based on client contractual requirements, relevant regulatory requirements, Avanade policies and CDP control standards. Develop action plans to close gaps.

**Implement Program and Close Gaps**
Implementation of the CDP program requires the creation of a formal CDP plan for the client that defines responsibility for all controls and confirms controls have been fully implemented.

**Monitor Compliance and Reassess**
Routine monitoring and auditing are conducted by independent teams that complete regular quality reviews and random compliance assessments to identify any control weaknesses and monitor corrective action.

**Client Data Protection (CDP) Control Categories**
The following list presents the security control categories that Avanade implements to protect our client data. It is by no means the full list of individual controls utilized by the Avanade CDP program. There are primary security controls with sub controls, as well as those required by the client and dependent on the client scope of work, such as a secure application development addendum for code development projects and Infrastructure Optimization (IO) for infrastructure hosting.

| Client Data Protection (CDP) Control Categories | |
|---|---|
| • Accountability | • Legal and Contractual |
| • Administrator Access | • Logging and Monitoring |
| • Approved Devices | • Movement of People |
| • Change Management | • Password Management |
| • Data Disposal | • Patching |
| • Database Backup | • Physical Security |
| • Delivery Locations | • Records Management |
| • Encryption | • Reuse of Work Products |
| • Environment Specific | • Secure App Development |
| • Firefighter IDs | • Security Incident Reporting |
| • Firewall and IDS/IPS | • Subcontractors |
| • HIPAA | • System Administration |
| • Infrastructure and Hosting | • Training |
| • Least Privileged Access | • Transmission of Data |

## CDP Program – Ongoing Audit and Compliance

Periodic assessments or audits are conducted to gauge the compliance and effectiveness of an active CDP plan and to improve the quality of Avanade's CDP plans overall. Plan owners are provided results with guidance and a 30-day remediation period to address the findings.

Three-month assessments are conducted by checking 10 high level areas of compliance with plan maintenance. These assessments measure short-term compliance and overall data protection behavior, and they provide a 'soft touch' check-in and learning tool for plan owners who need assistance with CDP requirements.

Six-month audits provide a deep review of contract compliance, control compliance and data protection behavior. Resource interviews, document reviews and full plan walk-throughs are included. Individual findings and the overall report are assigned a COSO rating of Green, Blue, Yellow or Red, based on the significance of the finding(s).

## Summary

Today's threat landscape continues to evolve with regard to complexity and emerging threats. To conduct business in the current threat landscape, Data Protection Protocols must be implemented to safeguard an organization's data and systems. Avanade is committed to protecting our clients' data. The Avanade Client Data Protection (CDP) program continues to undergo a continuous process improvement review, and the CDP team monitors the current threat landscape and emerging threats, so that security risks to our clients' business can be mitigated. To learn more about how Avanade's CDP program can help you protect your data and privacy during service delivery, contact your Avanade account team today.

## Authors:

Carl Almond, Senior Director, Global Avanade Asset & Data Protection
Sean Clark, Group Manager, Global Security Lead
David Cammon, Consultant, CDP Global Lead
Georgeo Pulikkathara, Director, Global Client Information Security Response
Larry A. Mathias, Group Manager, Security Sales Readiness Architect



North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Africa
Pretoria
Phone +27 12 622 4400
SouthAfrica@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
Asia-Pacific@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

[1] https://www.microsoft.com/en-us/security/intelligence-report
[2] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/