ENTERPRISE CRM: ETHICAL QUESTIONS AND TECHNICAL RESPONSIBILITIES

William Money
Robert J. Riggle
The Citadel

The Enterprise CRM firm produces, markets, and supports software to a wide variety of organizations and firms in the services arena. The case concerns ethical and responsibility questions faced by a contractor. The case provides an overview of Enterprise CRM, its CRM products, security, and the interaction between a contractor and a technology vendor. It reviews the information systems security concern for the industry, and the situation faced by the contractor. An overview of the security risks and sources for obtaining information about security threats and security risk data is included. The sources for these data are the firms producing software and services and the users working in the industry. The case summarizes the contractor's situation through emails exchanges, describes the threats observed by the contractor, and includes the interaction with the Enterprise CRM technical staff are presented. The case exposes the contractor's ethical concerns, and presents the contractor with an ethical decision about his personal position and responsibility to the customers and industry that uses the Enterprise CRM product. Students explore the decisions facing the contractor and the path he may choose to pursue or use to report on the security issue.

DOES KYLE WOODS CONTINUE?

Kyle Woods has received what appears to be another rebuff in his ongoing attempts to draw attention to a cybersecurity vulnerability he has found in a widely and frequently customer relationship management system (CRM). His quest to bring the vulnerability into the public domain and increase awareness has lasted for over 18 months. His goal has been to negotiate the path to awareness by working with the CRM vendor, without harming his relationship with the vendor and industry in which he works. He is well aware for the concerns and risks of cyber intrusions, and has a true fear for the clients he serves. At times, he questions his own ethics, and focus on this technical problem he has the uncovered. Should he persist with what, at times, feels somewhat like a crusade? Is he trying to protect the interests of the many users of CRM, and execute a true responsibility he has to customers that he ethically serves? If he simply drops this issue, is he walking away from what

he knows is a risk that he might be sued by a vendor for defaming them, or alternatively sued by a customer for failing in his duty to disclose what he knows about the systems and proprietary software solutions he supports?

ENTERPRISE CRM

Enterprise CRM is a Boston Massachusetts headquartered software firm. It is one of the leading competitor of cloud based CRM (customer relationship management) software as enterprise solutions. Its proprietary software solutions provide software applications that track customer data, services, marketing, automaton services, and analytics. The company also provides application development solutions through its platform. The company is highly regarded; Enterprise CRM ranks 31st in a recent business journal article as one of the "Most Attractive Companies to Work For" based on a worker survey of satisfaction.

The company's two founders were James Thompson, and Elizabeth Danes, a former leading software developer corporate executive. The business strategy was to design and sell software systems as services. In cloud terminology, this is a SaaS (software as a service) offering. The Enterprise CRM product is a cloud hosted software solution that offers ubiquitous, convenient, on-demand network access to a shared pool of configurable computing networks, servers, storage, applications, and services. The advantages of this computing service alternative are rapid access to more computing power and storage when required by a customer, limited management demands, and minimal need to the company providing the SaaS services. Customers use these systems without investing and supporting a development effort. The time to receive benefits from the system is shorter with software as a service (SaaS). It differs from the traditional model development model because the software (application) is complete, operational and configured. Other advantages of SaaS include lower total costs because the customer, data integration among various functional business areas, and the availability of new releases (automatic upgrades), does not maintain the software.

This cloud software services model is composed of five essential characteristics that benefit both the service (SaaS) provider and the clients. The needed computing services are available (and can be expanded) on-demand, are requested and granted on a self-service basis, provide broad network access, allow resource pooling (vendors can combine resources and efficiently serve multiple clients), and rapid expansion of the resources to meet the client's demands. Measured service), three service models Software as a Service (SaaS).

The Enterprise CRM year history is complex. It involves many acquisitions and business model evolutionary steps. Exhibit 1 presents the corporate history of the firm for a 16-year period.

EXHIBIT 1

ENTERPRISE CRM, INC. FINANCIAL STATEMENTS 2006-2021 REPORTED REVENUES, NET INCOME, ASSETS AND PRICE PER SHARE, AND EMPLOYEES

Year	Revenue US$ millions	Net income US$ millions	Total Assets US$ millions	Price per Share US$	Employees
2006	155	3	206	4.01	367
2007	301	14	411	6.52	1,094
2008	382	4	555	8.90	1,698
2009	539	29	780	10.80	2,590
2010	866	31	1,003	11.03	3,005
2011	932	44	1,631	18.56	3345
2012	1,003	54	1,819	22.08	4,108
2013	1,457	-42	2,216	31.97	5,075
2014	2,143	-140	4,319	39.84	6,980
2015	2,665	-122	6,013	48.06	9,112
2016	3,462	-63	7,764	59.60	11,812
2017	4,993	8	10,313	71.70	14,213
2018	6,452	221	12,658	77.32	18,012
2019	8,261	411	17,809	101.70	21,730
2020	9,783	810	22,624	121.90	24,122
2021	11,881	936	28,445		28,000

EXHIBIT 2

ENTERPRISE CRM TOOL INSTALLATIONS

	Tree Package Manager (*weekly downloads*)	VS Code Marketplace (*installations*)
@Enterprise/base	284,933	845,640

KYLE M. WOODS

Mr. Kyle Woods is an Enterprise Cloud Architect and software consultant with over 25 years of experience in technology across multiple platforms with multiple software vendors. He provides enterprise level system consulting and implementation services to the Federal Government, Department of Defense, commercial entities as well as non-profit organizations. He is not and has never been an employee of Enterprise CRM. Mr. Woods consults directly with Enterprise CRM customers, counsels, stakeholders, and mentors software engineering delivery teams with current relevant delivery and software implementation techniques. Kyle holds 12 current Enterprise CRM Certifications including Certified Enterprise CRM Architect and Certified Access Management and Identity Architect. He is a very capable developer, and codes in a number of different software languages. He received his Master of Science in Computers and Information Systems from a major research university and holds a number of other industry certifications.

Kyle is highly concerned because he has found what he believes is a significant vulnerability with a common Enterprise CRM software tool. This tool is frequently used by Enterprise CRM Administrators and Developers who support and add tailored reporting and user specific feature to the Enterprise CRM products.

Kyle carefully studied the Enterprise CRM security issues that are addressed by Enterprise CRM, Inc. on their website and in supporting documentation and an Enterprise CRM Security Inspection Instructions and Documentation white paper that only addresses replication and guarding against data lost utilizing the Enterprise CRM cloud environment. It includes a replication concept to protect users against disaster, and to recover data. This proposal did not address privacy, reliability, and security.

He did not find a resolution or recognition of the cybersecurity threat he found in this document. This, he sent the following email text to the Enterprise CRM Information Security team.

The following code will give someone "keys to the castle" to manipulate one or more orgs using typescript or JavaScript. Using the IdentInfo.create' method with

a valid authenticated usernameOrAlias will return a decrypted AuthInfo object and a valid decrypted security token.

The example here is what I use to access my dev org. There are several issues:

1. IdentInfo.create returns a decrypted accessToken
2. ecrm crm:inst:print also returns a decrypted accessToken

A programmer can use the @enterprise-crm/base module to access the token directly, but a simple scrape of a shell terminal will also give access to a security token.

All of the authorized user info is stored at rest in a hidden directory. Removing the .json extension will give someone the ability to create a project stub, login and automatically execute code such as the tooling api, the various rest apis and the Scripting Soap API. (Copy of the code and instructions was inserted here)

This represents a significant vulnerability that can be leveraged by bad actors.

Regards,

Kyle

Enterprise CRM Information Security replied:

Hi,

Thank you for contacting Enterprise CRM.
The report should include more context. It looks like this is running in VSCode, possibly as an extension? Moreover, it reads either credentials or a saved access token from the file system, possibly performs a log in, and displays the results.
The "keys to the castle" aren't the access token, they're the credentials you use to obtain it.

Please provide more detail about what the environment of this attack is, and what is necessary to set it up.

Please follow the steps outlined in Security Vulnerability Finding Submittal Guide to report the security vulnerability to Enterprise CRM.

Please include as much information as possible to help us better understand the nature and scope of the reported issue (replication steps with the proof of concept demonstrating each vulnerability, HTTP Request/Response, screenshots, payload, etc.).

Regards,

Enterprise CRM | Enterprise Software Security Incident Answer Team
security@EnterpriseCRM.com

Several email exchanges followed over the next 18 months.

Kyle included a further technical description and the example of the suspect code and stated:
"I beg you to consider the implications on this simple PowerShell Script:…(script code was included), and there are a ton of federal projects depending on the CLI and good security. The Token issue could wreak havoc on projects. Please, I beg you to reconsider the rendering of unencrypted tokens. Ask yourself which desktop apps with Super User Capabilities and OAuth render tokens to users."

Enterprise CRM responded to this email with:
We can continue the conversation on there for now. If we need to drive more conversation around it, can you file a support ticket so I can track the conversation on our end?

In a final email exchange, Kyle again reported having discovered a vulnerability in an Enterprise CRM desktop tool (Enterprise CLI). He emphasized that this vulnerability can be exploited to gain access to live administrator/developer Access tokens (Session Id's) and Refresh tokens and noted that this tool is being used by several Federal Agencies and possibly one or more Department of Defense application teams. His description of the problem stated that the session Id shared by this tool will bypass multifactor authentication (MFA) and can be used by a threat actor to access the Enterprise CRM GUI and the more powerful Enterprise

CRM API's. The Enterprise CRM API's with a stolen session Id are capable of exporting Enterprise CRM Data, Code and Users for affected Federal, Commercial and DoD systems.

Kyle concluded his email reply by asking, "What process (es) do you recommend for vetting my findings and disseminating the vulnerability to affect parties?"

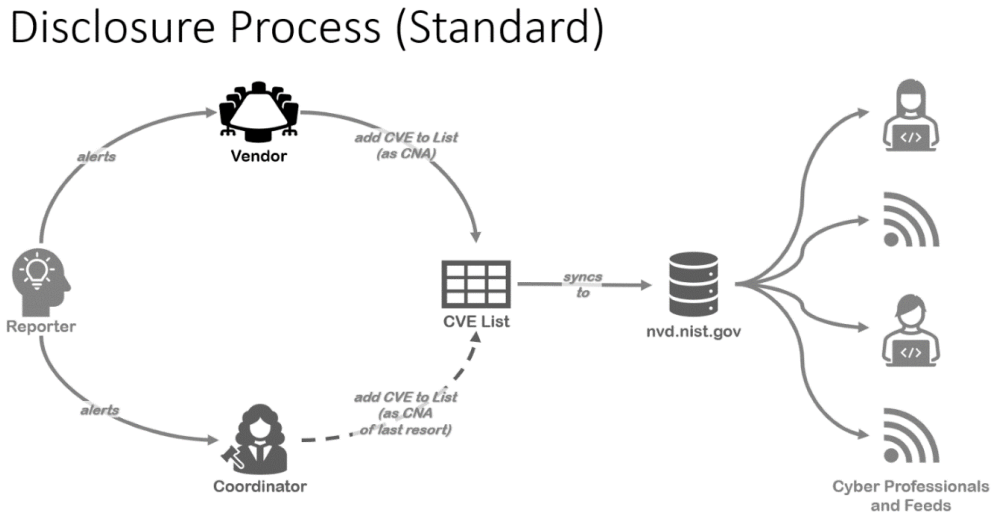
REFLECTION

Kyle's lengthy experience with Enterprise CRM products and training give him confidence that he is seeing one or more threats for client and system exposures and security breaches. However, this extended exchange of emails and data with Enterprise CRM security and support staff has led him to question his own thinking and findings. For his own "comfort level," he consulted personally with several very knowledgeable security sources including vendor certified architects and industry recognized cybersecurity professionals. Kyle knows that these individuals have lengthy work experience, and technical familiarity with information systems security and vulnerability in other firms and situations. The responses he received reassured Kyle that his findings were technically correct. He believes (more strongly than ever) that the cybersecurity vulnerability could be used to access the credentials of system users as Kyle has indicated.

TAKING ACTION AND REACHING OUT

Kyle has investigated security vulnerability reporting. He understands that there is no unique or single security or vulnerability listing addressing the threats and vulnerabilities of tools used in the software services industry. Thus, vulnerabilities may or may not be reported in different locations and to several different public and private organizations. In general, the cybersecurity teams within these report-collecting organizations seek to improve the security of computer systems and communication networks by collecting and analyzing problems that may have software and cybersecurity consequences. The organizations function by publishing coordinated (but not necessarily comprehensive) lists of Common Vulnerabilities and Exposures (CVE) registered in a database of publicly disclosed computer security flaws. The diagram in Figure 1 presents a diagram of the overall disclosure process. It shows the dual alerting processes, and the eventual addition of an alert to a database that may be accessed by a user.

FIGURE 1
DISCLOSURE PROCESS (STANDARD)



Kyle has used this process to alter the collecting and reporting organizations about the Enterprise CRM vulnerability. He independently reported the discovered vulnerability to three different organizations that collect, test, track and communicate software vulnerabilities by sending them the data he previously submitted to Enterprise CRM. He is aware that these cybersecurity teams in these organizations include researchers, software engineers, security analysts, and digital intelligence specialists who assess software product cybersecurity vulnerabilities. To his dismay, these organizations have expressed no interest in obtaining any information from Kyle and have not reported or listed a vulnerability that is similar to or associated with Kyle's communications.

THE CURRENT STATE OF AFFAIRS

Enterprise CRM has recently acknowledged Kyle's concern in Information Report 0001763541: "Setting Up the Enterprise CRM Developer Experience Command Line Interface" and posted their article response on https://help.EnterpriseCRM.com/. There posted documentation state:

"The default configuration in Enterprise CRM Base allows an authenticated user with an Enterprise CRM CLI (available with the Spring '19 release) to create a

URL that would enable any user to access Enterprise CRM services with the same rights, without a log trace of access. A malicious user with access to the URL could perform administrative actions on behalf of the account owner who generated the token."

Kyle is surprised and disheartened by this acknowledgement. His personal opinion is that that the announcement simply places the entire burden of avoiding this threat and (if they choose) attempting to fix the vulnerability on the user.

THE VALUE IN CRM

Kyle has a deep understanding of the value and importance of CRM, and the cybersecurity risk posed if the data and proprietary customer information in the databases of a CRM system are compromised. Enterprise CRM is a CRM (Customer Relationship Management) company providing essential services to many organizations that obtain great value from understanding their customer's needs and interests, purchases and opinions. The growth in this industry and interests in the software is attributed to the important services provided to the users. A wide variety of industries are obtaining CRM's value from using CRM in disciplined, focused ways to realize the benefits. CRM services and applications are addressing and solving highly specific customer-relationship tasks. They are used to diagnose call center customers' problems and obtain timely information where it is valuable in the organization.

Examples of CRTM value include real-time data showing room availability for hotel management. CRM gained a positive reputation and became valuable when it was applied to successful smaller CRM projects. These applications then contributed to the solutions to larger problems that would improve revenue gains in companies like Kimberly-Clark, Ingersoll-Rand, and Brother. Aviall Inc., Aircraft-parts distributor, sought to become a premier provider of supply-chain management services by developing a highly trained sales force. It improved sales-force and order-entry productivity with specific CRM software products that delivered instant access to customers' credit history, a streamlined order-processing system. This information enabled the sales staff to provide immediate firm quotes. The impact of the company was significant. The number of daily sales calls tripled and the customer base expanded by one-third. Actual orders handled daily more than doubled without adding staff. The impact extended to the corporate level

because the company successfully won a supply contract from engine maker Rolls-Royce for ten-years and $3 billion.

The CRM impact on a firm's value chain is at the heart of the CRM benefit. CRM is closely related to how both marketing and communication enabled by information technology. It is a service, a highly sophisticated sales function that is fundamentally an enabler of a 1 to 1 communication environment. The 1 to 1 relationship exists between the service provider (organization with products and services) and the customer. It has been conceptualized it as a strategic process using data and software to answer questions such as who, what and how a company can serve customers. In this sense, it also affects many other functional areas of the organization such as HR, R&D and finance.

This view of CRM is that it is a value chain enabling process. It ensures that long-term mutually beneficial relationships develop with customers. A key of CRM's is its value in helping the organization focus on customers that are strategically significant to the organization. Those less important customers that buy little or have infrequent interactions that are not deemed significant or strategic. These may be customers that have characteristics or behaviors that do not favor the organization such as paying late, defaulting or agreements, or requests that impose extraordinary demands on customer service and sales departments. They may also seek special treatments, customized outputs; and move to competitors. The CRM solution can aid in identifying strategically significant customers that are essential to the organization, and demand attention for customer retention. CRM analytics may aid the organization in assessing the lifetime value potential of the customer. This is the present-day value of all future margins that might be earned in a relationship.

Simply stated, the result of effectively utilized CRM data to provide intelligence to a firm. They note that CRM databases have grown to be massive data libraries in the form of sophisticated relational databases. However, in many cases these data are not well utilized due to the limited understanding managers have of the data and poor data management. Managers must actively guide the development of processes and tools to more effectively utilize CRM data for sophisticated market analysis.

Management must analyze the data across market segments, customer categories, and various customer–firm relationship forms. This will enable management to make decisions based upon meaningful conclusions. This requires classification of the CRM information to guide management decisions leading to improved understandings of the in-forming process in the firm's dealings with its clients. It will also contribute to understanding the directionality of customer–firm decision-making, identifying key decision drivers, and document the historical record of the firm's customer relationship. This establishes competitive strategies that can expand the firm's customer base with effective policies and programs.

Constant improvements in the application of CRM and data are found in the use of AI for CRM purposes today. Artificial intelligence (AI) has been viewed as affecting CRM capabilities. AI capabilities are projected to transform CRM by influencing the customer acquisition, development, and retention processes. CRM's will utilize and incorporate AI to better predict customer lifetime value and support the implementation of the adapted treatment of customers. This use of AI will contribute to greater customer prioritization and market service discrimination. The mechanisms for this CRM and AI combination may also be understood by the smart customer. CRM customers could also strategically leverage AI's by learning how to better negotiate and use their personal data as a strategic advantage by shifting value capture away from firms. Thus, AI can enable organizations to better discriminate among customers and avoid wasting superior customer service or higher quality products to customers who do not "deserve" this treatment. Thus, AI may assist other customers to decompose the decision rules applied and manipulate the inputs to those rules to their benefit. This counter-strategizing could see both discrimination favoring the "best" customer, and "best" customers learning how to utilize the CRM strategies to their advantage.

Collection of CRM data from multiple locations and devices has led to locating storage, and analytical resources toward the edges of networks. This essentially means that the storage and analysis is placed closer to the collection devices (reducing in-cloud storage, bandwidth requirements. Fog computing demands less immediate cloud storage enabling rapid strategic compilation and distribution for improved efficiency and reduced costs. Improved user experience and reduces burdens on the cloud improving the uses of data from the IoT.

CRM AND SECURITY

Kyle also appreciates (and fears for his clients) because he understands the enormous risk of growing cybersecurity threats and attacks. CRM data present a large target for cyber security attackers. All organizations are very vulnerable to cybercriminals and numerous types of security attacks. However, successful attacks of the large databases can lead to the potential loss of private client and business information. Data can be stolen and strategically used against the organization or released and thereby threaten clients and partnering business with further attacks, expensive recovery operations, embarrassment and loss of the customer. Notable newspaper and internet published headline-grabbing attacks are important, but understate the additional dangers exist from infiltration and network attacks, and ransomware. In this instance, then the operating system is hacked, money (or crypto currency) is demanded in large sums for a business or individual to obtain an encryption key to "free" the data.

There are no easy solutions to the security threats and attacks. It is important to share detailed information on how adversaries tried or succeeded in breaching us to help patch systems or change procedures to thwart the attacks or by exchanging detailed actionable information. However, this approach only enables one to prevent "what you or others have seen." It does not implement complete prevention or implement the actions to isolate the infected machine or slowing down network activity until a human is available to assess the breach. The need for better information has been recognized for a number of years. An article published by Cisco states "President Obama's call for a 30-day mandatory disclosure of retail data breaches in his 2015 State of the Union address illustrates the gravity of such security failures, felt even at the highest levels of government."

Some large organizations, like Target, have their own security operations centers. Their center located in Minneapolis, Minnesota also relies on a team in India to monitor their systems. During Thanksgiving of 2013, suspicious behavior was identified and reported to the security operations center, but was ignored by management. This resulted in information of more than 110 million Target customers to be stolen. It was noted that Target seemed to ignore warnings and never followed what was assumed proper protocol at their security operations center.

A literature review identifies the major vulnerabilities associated with CRM systems. The possible types of attacks included: 1) denial of service (DOS) that makes an attacked system inaccessible to customers; 2) intrusion into sales automation systems and customer database accessing customer information; 3) identity theft – when attackers use personal information without your permission to commit fraud or other crimes; 4) malware attacks with viruses and worms causing systems and, hardware damage and data loss or a denial of service.

The importance of ensuring security in CRM systems is not fully understood by users. However, research investigated the micro-linkages between electronic customer relationship management (E-CRM) and electronic loyalty of customers in the field of electronic banking satisfaction. It found a significant correlation between E- CRM expected security and customer intentions of repeat e-dealing and providing customer's positive feedback to others. The limited findings suggest that customer's loyalty is likely to increase when technological protection mechanisms for electronic banking transactions are provided.

HOW SECURITY INFORMATION AND COMMUNICATION IS MAINTAINED IN THE SOFTWARE INDUSTY

Finally, Kyle is all too familiar with how security vulnerabilities are exploited by Malware and other software attack-tools that take advantage of these known vectors for attacking systems. He has studied how Heartbleed attacked with a vulnerability in the OpenSSL code. WannaCry used a security vulnerability in the Microsoft Windows SMB protocol, and SolarWinds hack inserted malicious code into the Orion version of update software. These attacks and the damage done by the attacks are described in many trade articles.

THE DECISIONS

Kyle is facing a complex decision about how to assess and continue (or halt) his attempts to draw attention to the cybersecurity risk he believes exists within Enterprise CRM. He believes that he has a responsibility to his clients to protect their interests, and to identify cyber security threats. Should he continue to report his findings to Enterprise CRM, and repeatedly press this issue? He suspect that his communications and exchanges with Enterprise CRM, and the final notice they have posted mean that the company does not intend to offer a solution to the threat. However, he cannot be certain of this. The company might be "buying time" and intend to fix the problem is some future release. In either case, the vulnerability is

there now. Should he report the vulnerability to his customers and press them regarding changes they should make to protect their systems

He knows that he has a very significant stake in the success of salesforce and the protection of customer's security handle this situation. Perhaps it is time to stop this entire effort. Enterprise CRM may take some action against him because his communications could negatively affect sales. This could force him "out of his consulting business" and ruin him if he had to defend himself in a lawsuit.

Finally, should he collect more evidence and documentation on the threat, and develop more detailed examples that can be submitted to the organizations that may report and track cybersecurity problems. In a similar publication attempt, should he continue his attempts to communicate this information and prove his case to other third party researchers, designers and developers? Alternatively, should he "go public?" The analysis data and description of the problem could be sent to widely distributed industry publications and internet sites. His understanding of the nature of the threat, and risks involved in the situation is extensive and the details could show possible hackers and others a new attack vector for Enterprise CRM.

What is next for Kyle?