STATE OF MICHIGAN

COURT OF APPEALS

PEOPLE OF THE STATE OF MICHIGAN, Plaintiff-Appellee,	UNPUBLISHED May 3, 2005
v	No. 253117 Oakland Circuit Court
VALRENE MAE SCHILKE, Defendant-Appellant.	LC No. 2003-189729-FH

Before: Saad, P.J., and Fitzgerald and Smolenski, JJ.

PER CURIAM.

A jury convicted defendant Valrene Mae Schilke of one count of unauthorized access to a computer.[1] The trial court sentenced defendant to a three-year term of probation with the first 183 days to be served in jail. The trial court also ordered defendant to pay restitution in the amount of $36,591.01. Defendant appeals her conviction and sentence, and we affirm.

I

Express Management Services ("EMS") is a company that performs data imaging for financial services companies.[2] EMS employed defendant as a "technical analyst." In this position, defendant was responsible for the maintenance of EMS's computer network. In this capacity, she had "administrative" access to the network, as well as the "administrator password"[3] for the system. She also had access, but not authorization, to establish a "virtual private network" (VPN) to connect to the network remotely from her home computer.

On December 9, 2002, Laura Sclesky, defendant's supervisor, and Clara Loria, EMS's human resources director, went to defendant's office to notify defendant that EMS was

[1] MCL 752.795.

[2] For example, banks would send EMS mortgage loan documents for scanning and electronic imaging.

[3] The "administrator password" can be thought of as a sort of "master key" for a network, and it allows complete, unfettered access to the network, including the power to add and delete users and files, and the ability to grant and revoke access privileges to other users of the network.

terminating defendant's employment. Defendant sat facing her computer with her back to Sclesky and Loria, and did not look at them. After she was told that her employment was terminated, defendant continued to type. Loria told defendant to stop typing, and defendant replied, "if you're going to f--- me, I'm going to f--- you," and continued to type. Sclesky and Loria left defendant's office in an attempt to get someone to disconnect defendant's computer from the network, and when they returned, defendant's office door was closed and was barricaded so that no one could enter. EMS called the police; after the police arrived, defendant left her office, and the police escorted her out of the building and to her car.

EMS employee James Coe was asked to disconnect defendant's computer from the EMS network. Before defendant learned she was terminated, Coe had been able to access the network using the administrative password. Shortly after defendant was fired, he was unable to use the same password. After defendant left EMS property, Coe saw that someone was attempting to remotely access the network. Coe unsuccessfully tried to block this remote access attempt, and finally pulled the power plug to the server to prevent access. After spending the next twenty hours restoring the system, Coe discovered that all but three of the network user accounts had been deleted. The three remaining accounts were the administrator account, defendant's account, and a third, normally low-level account that had been given administrative access by defendant to provide her with a "back door" to the system. Coe also discovered that several computer disk drive designations had been changed and that the event log[4] had been deleted. A significant amount of data being processed at the time of this incident was lost as well. The event log, however, had recorded several attempts to log into EMS's network remotely. The Internet Protocol (IP) address number was traced back to defendant's home computer.

Detective James Mork of the Troy Police Department testified that he executed a search warrant at defendant's home. Detective Mork testified that defendant admitted to changing the administrative password and deleting user accounts after her employment was terminated. Defendant also admitted to Detective Mork that she was in possession of several tapes and compact discs that contained backup and customer loan information from EMS.

At trial, defendant admitted that she changed the administrative password, deleted user accounts, and took home backup tapes and CDs without authorization. She denied that she deleted the event log or changed the disc drive designations. Defendant claimed that she left her computer workstation at EMS turned on so that EMS personnel could change the administrative password. She also claimed that she planned to give an EMS employee the new administrative password, but admitted that she never did so.

II

Defendant argues that the trial court erred when it admitted evidence relating to the amount of money EMS spent repairing the network, and the amount of lost revenue arising out of EMS's inability to conduct business due to the unavailability of the network. We review a trial court's decision to admit evidence for an abuse of discretion. *People v Matuszak*, 263 Mich

[4] This is a computer file that records certain actions taken on a computer system.

App 42, 47; 687 NW2d 342 (2004). To be admissible, evidence must be relevant. MRE 401, 402. Evidence that is substantially more prejudicial than probative may be excluded. MRE 403. Reversal based upon an error in the admission of evidence is not warranted where that error is harmless. *People v Ullah*, 216 Mich App 669; 550 NW2d 568 (1996).

Here, defendant argues that testimony that showed EMS paid in excess of $11,000 to restore its network, and had a loss in revenue of approximately $48,000, was not relevant because the amount of damage is not an element of the crime. Moreover, defendant argues that such evidence, if relevant, is substantially more prejudicial than probative. Defendant likens the evidence to pictures of a grisly murder scene that can only serve to inflame the jury.

MCL 752.795 provides:

> A person shall not intentionally and without authorization or by exceeding valid authorization do any of the following:
>
> (a) Access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, *alter*, *damage*, *delete*, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network. [MCL 752.795(a) (emphasis added).]

Though the amount of damage sustained is not an element of the charged crime here, the fact of that damage is. The challenged testimony was relevant to the question of whether EMS sustained damage to its computer network and the challenged evidence reflected defendant's defense. That is, at trial, defendant claimed that her actions should have been easily correctable, and should not have caused very much damage. Obviously, the damage evidence is relevant to rebut this assertion.[5]

Accordingly, we hold that the trial court did not abuse its discretion when it admitted the challenged evidence.

III

Defendant maintains that the trial court erroneously refused to take judicial notice of information located at Microsoft's web site regarding the corruption of event log files on Microsoft servers. MRE 201 provides:

> A judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2)

[5] Moreover, were we to hold that the admission of this evidence was erroneous, which we do not, we would nevertheless hold that any error is harmless. Defendant admitted that, after her employment was terminated, she changed the administrative password and deleted user accounts. This more than satisfied the "alter" and "delete" elements of the statute.

> capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. [MRE 201(b).]

Here, defendant claimed at trial that she did not delete the event log on EMS's network, but rather, that a known defect in Microsoft's server was instead responsible for the missing information. She asked the trial court to take judicial notice of information on the Microsoft web site that documented this issue. The trial court ruled that it could not simply accept information contained on the web site as being accurate without expert testimony, and it therefore refused to take judicial notice of this information.

Because the alleged problem with event logs is not "capable of accurate and ready determination," and because we agree with the trial court that the Microsoft web site does not constitute a "source[] whose accuracy cannot be reasonably questioned," we hold that the trial court did not err when it declined to take judicial notice of information contained at the Microsoft web site.

Affirmed.

/s/ Henry William Saad
/s/ E. Thomas Fitzgerald
/s/ Michael R. Smolenski