

# PCGenesis

## Ransomware Attacks and Backing Up PCGenesis

**GASBO**

**Augusta, GA**

**November 9, 2022**

# Agenda

- **Introduction**
- Backing Up PCGenesis
- PCGenesis Server Requirements
- Ransomware Attacks
- PCGenesis Broadcast E-mail List



# Ransomware Attacks and Backing Up PCGenesis

## PCGenesis Team

Steven Roache	Director, Applications Development
Diane Ochala	PCGenesis Lead Analyst/Developer
Angela Tennyson	PCGenesis Senior Developer
Karen McArthur	PCGenesis Developer
Katie Green	Data Collection Specialist
Stephanie Smith	Data Collections

# PCGenesis Sessions/Training at GASBO

- **Session 2 – 10:00** *Wed 11/9/2022*
  - **Ransomware Attacks and Backing Up PCGenesis**
- **Session 3 – 11:00** *Wed 11/9/2022*
  - PCGenesis and the CPI Process
- **Session 4 – 2:10** *Wed 11/9/2022*
  - Payroll for Beginners
- **Session 5 – 3:30** *Wed 11/9/2022*
  - PCGenesis Budget System Overview
- **Session 6 – 9:00** *Thur 11/10/2022*
  - PCGenesis Budget System Gross Data, Budget Flag, Salary Schedules
- **Session 7– 10:20** *Thur 11/10/2022*
  - PCGenesis Budget System Playing in the Sandbox
- **Session 8 – 11:20** *Thur 11/10/2022*
  - PCGenesis Budget System Create Final Budget

# Agenda

- Introduction
- **Backing Up PCGenesis**
- PCGenesis Server Requirements
- Ransomware Attacks
- PCGenesis Broadcast E-mail List



# Ransomware Attacks and Backing Up PCGenesis

Where is most PCGenesis production data stored today?

# Ransomware Attacks and Backing Up PCGenesis

Where is most PCGenesis production data stored today?

~~K:\SECOND~~

# Ransomware Attacks and Backing Up PCGenesis

Where is most PCGenesis production data stored today?

~~K:\SECOND~~

K:\PCGSQldb 



# Ransomware Attacks and Backing Up PCGenesis

Who is going to have to make up the work if your school district has a ransomware attack and **K:\PCGSQldb** is not backed up?

# Ransomware Attacks and Backing Up PCGenesis

Whose best interest is it to make sure that the **K:\PCGSQldb** directory is on your backup media?

# Ransomware Attacks and Backing Up PCGenesis

It does absolutely no good if K:\SECOND is on the backup, but **K:\PCGSQldb** is not!

- All of your recent financial data is gone!
- All of your recent payroll data is gone!
- All of your recent CPI data is gone!

# Ransomware Attacks and Backing Up PCGenesis

- **K:\SECOND** cannot be restored without also restoring the **PCGenesisDB** database.
- These two entities must be kept in sync, otherwise financial and payroll postings may be lost

# Ransomware Attacks and Backing Up PCGenesis

- The help desk has worked with multiple school districts that realize **AFTER** a ransomware attack that they were not getting **K:\PCGSQldb** copied to a backup!
- This is all too common!

# Ransomware Attacks and Backing Up PCGenesis

- It has taken everybody involved hours, days, and weeks to recover data.
- Is payroll going to be ready in time if you have to recover?!

# Ransomware Attacks and Backing Up PCGenesis

Why is **K:\PCGSQldb** not on the backup media?

1. **PCGSQldb** was never added to the list of directories to backup
2. Most items in **PCGSQldb** can't be backed up until Microsoft SQLServer is not actively running

# Ransomware Attacks and Backing Up PCGenesis

Prior to running a backup of the **K:\PCGSQldb** directory:

- School districts must stop these services for the backup to successfully run to completion:
  - *VerraDyne Queue Service*
  - **SQL Server (SQLEXPRESS)**



# Ransomware Attacks and Backing Up PCGenesis

Prior to running a backup of the **K:\PCGSQldb** directory:

- The following commands should be added to the backup bat file to stop the services:
  - **NET STOP VQueueService**
  - **NET STOP MSSQL\$SQLEXPRESSPCG**

# Ransomware Attacks and Backing Up PCGenesis

After the **K:\PCGSQldb** directory backup has completed – Start Services:

- The following commands should be added to the backup bat file to start the services:
  - **NET START MSSQL\$SQLEXPRESSPCG**

# Ransomware Attacks and Backing Up PCGenesis

After the **K:\PCGSQldb** directory backup has completed – Start Services:

- **NET START VQueueService**

(Make sure to **wait at least 2 minutes** for **SQLEXPRESSPCG** to start before trying to start **VQueueService**)

# Ransomware Attacks and Backing Up PCGenesis

Make your IT department **VERIFY** your backup!

# Ransomware Attacks and Backing Up PCGenesis

## Technical System Operations Guide

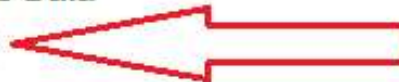
---

### Section A: PCGenesis Configuration

- Topic 1: New Server Installation Checklist
- Topic 2: New Workstation Installation Checklist
- Topic 3: Setting Windows® Server Environment Variables
- Topic 4: Microsoft SQL Server Express 2016 Installation Instructions
- Topic 5: MyGaDOE Helpdesk Portal Basics
- Topic 6: MyGaDOE Portal Message Center

### Section B: PCGenesis Backup / Reorganization / Restore

- Topic 1: PCGenesis Backup / Reorganization / Restore Checklist
- Topic 2: How To Schedule the PCGenesis Reorganization Job
- Topic 3: Adhoc Backup/Restore for PCGenesis Data
- Topic 4: How to Verify the PCGenesis Backup



# Ransomware Attacks and Backing Up PCGenesis

**What you need for a disaster recovery:**

- **K:\PCGSQldb**
- **K:\SECOND**

# Ransomware Attacks and Backing Up PCGenesis

## What you need for a disaster recovery:

- **K:\PCGSQldb**
- **K:\SECOND**
- Verify that these two directories are on your backup media – at a minimum

# Ransomware Attacks and Backing Up PCGenesis

Let's take a look at **K:\PCGSQldb...**









- Drill down a couple of levels:
  - **MSSQL13.SQLEXPRESSPCG**
  - **MSSQL**



# Ransomware Attacks and Backing Up PCGenesis

Let's take a look at **K:\PCGSQldb...**

PCGSQldb > MSSQL13.SQLEXPRESSPCG > MSSQL >

Name	Date modified	Type
 Backup	9/16/2022 11:52 AM	File folder
 Binn	8/24/2022 12:12 PM	File folder
 DATA	9/28/2022 1:54 PM	File folder
 Install	8/24/2022 12:12 PM	File folder
 JOBS	10/13/2021 3:52 PM	File folder
 Log	9/29/2022 6:37 PM	File folder
 Template Data	8/24/2022 12:12 PM	File folder
 sql_engine_core_inst_keyfile.dll	10/29/2016 5:20 AM	Application exten...

# Ransomware Attacks and Backing Up PCGenesis

Let's take a look at **K:\PCGSQldb...**

- Two of these directories are important:
  - **BACKUP**
  - **DATA**

# Ransomware Attacks and Backing Up PCGenesis

Let's take a look at **K:\PCGSQldb...**

- Two of these directories are important:
  - **BACKUP** – System restore points
  - **DATA**

# Ransomware Attacks and Backing Up PCGenesis

Let's take a look at **K:\PCGSQldb...**

- Two of these directories are important:
  - **BACKUP** – System restore points
  - **DATA** – Production data

# Ransomware Attacks and Backing Up PCGenesis

Let's take a look at **K:\PCGSQldb...**

- Two of these directories are important:
  - **BACKUP** – System restore points
  - **DATA** – Production data
- These directories better be on your backup media!

# PCGenesis Databases - Backup

- New feature!
- Adhoc Backup/Restore Option for PCGenesis Data
- On the ***System Utilities Menu***
- ***Backup / Restore PCGenesis Data*** (F30, F12).

# PCGenesis Databases - Backup

- ***Backup / Restore PCGenesis Data*** (F30, F12).
- This is a quick and easy way to get a backup!
- Backs up the important PCGenesis data.

# PCGenesis Databases - Backup

PCG Dist=8991 Rel=19.03.00 10/03/2019 PCG 001 SV C:\DEVSY S C:\SECOND WHITE

**Backup/Restore PCGenesis Data**

Select Type:  Backup PCGenesis Data  
 Restore PCGenesis DB  
 Restore PCGenesis Schema

Must call the HELP DESK to restore.  
Restore requires the DOE password.

ENTER = Continue, F16 = Exit

19.03.00



# PCGenesis Databases - Backup

PCG Dist=8991 Rel=19.03.00 10/03/2019 PCG 001 SV C:\DEVSYS C:\SECOND WHITE

BACKUPCG

Backup/Restore PCGenesis Data

Select Type:

- Backup PCGenesis Data
- Restore PCGenesis DB
- Restore PCGenesis Schema

ENTER = Continue, F16 = Exit

ENTER ✓

F16 ←

19.03.00

Backup can be run by anyone as needed!  
Both **PCGenesisDB** and **K:\SECOND** are backed up

# PCGenesis Databases - Backup

PCG Dist=8991 Rel=19.03.00 10/03/2019 PCG 001 SV C:\DEVSY S C:\SECOND WHITE

**BACKUPCG**

\*\*\* WARNING \*\*\*

\*\*\* BACKUP \*\*\*

\*\* This process will backup PCGENESISDB to PCGENESISDBx, where x \*\*  
\*\* is a letter A - K. \*\*

\*\* \*\*

\*\* K:\PCGSQLdb\MSSQLnn.SQLEXPRESSPCG\MSSQL\Backup\PCGENESISDBx.BAK \*\*

\*\* \*\*

\*\* This process will also backup SECOND to SECONdx. Make sure \*\*

\*\* all users are logged out of the system before proceeding. \*\*

A Enter a letter A thru K

**Pick a letter A thru K**

\*\* Press ENTER to Continue \*\*

\*\* Press F16 to Exit \*\*

ENTER ✓

F16 ←

19.03.00

# PCGenesis Databases - Backup

PCGSQLdb > MSSQL13.SQLEXPRESSPCG > MSSQL > Backup

Name	Date modified	Type
PCGenesisDBA.BAK	10/3/2019 10:28 AM	BAK File
PCGene DBJ.BAK	8/29/2019 7:55 PM	BAK File
PCG DBL.BAK	9/30/2019 2:53 PM	BAK File
P DBQ.BAK	9/30/2019 4:07 PM	BAK File
DBX.BAK	10/3/2019 1:01 AM	BAK File
3.bak	1/7/2019 3:03 PM	BAK File

Used '**A**' for backup:

Creates **PCGenesisDBA.BAK** in **Backup** folder

This is a backup of the database!

# PCGenesis Databases - Backup

Name	Date modified	Type
ACUCBL	5/23/2019 8:57 AM	File folder
Backup	6/24/2019 12:28 PM	File folder
etc	5/24/2019 10:00 A...	File folder
INS	6/24/2019 12:28 PM	File folder
INS19200	6/24/2019 12:28 PM	File folder
INSTAL	6/24/2019 12:28 PM	File folder
PCGIcon	10/1/2019 3:08 PM	File folder
PCGSQLdb	5/23/2019 2:24 PM	File folder
Restore	6/24/2019 12:24 PM	File folder
SECOND	9/30/2019 3:31 PM	File folder
<b>SECONDA</b>	10/3/2019 10:35 A...	File folder
SECONDL	5/24/2019 10:09 A...	File folder
SYSTEM	6/24/2019 12:28 PM	File folder
UCTARCHIVE	2019 9:51 AM	File folder
UCTPRINT		
Uniacu		
UTILITY		
vqueue		

Used 'A' for backup:  
Creates **K:\SECONDA** folder  
This is a backup of the **SECOND** data!

# PCGenesis Databases - Backup

Now *you* have control of your backup:

1. Zip K:\SECONDx → **SECONDx.zip**
2. Locate PCGenesisDBx.BAK in  
K:\PCGSQldb\MSSQL13.SQLEXPRESSPCG\MSSQL\Backup
3. Copy PCGenesisDBx.BAK to root of K:
4. Zip K:\PCGenesisDBx.BAK →  
**PCGenesisDBx.BAK.zip**
5. Copy both zip files to USB drive
6. You have your own backup of your data!

# PCGenesis Databases - Backup

If you put your backup on a small storage device like USB:

- Remember this backup contains sensitive payroll data
- Make sure to keep your storage device in a **secure location!**
- Don't store in desk drawers, pockets, backpacks, purses, etc.

# Agenda

- Introduction
- Backing Up PCGenesis
- **PCGenesis Server Requirements**
- Ransomware Attacks
- PCGenesis Broadcast E-mail List



# PCGenesis Server Requirements

## Supported Windows Server Versions:

- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Workstation Windows 8 and Windows 10 are supported

- Windows 11 coming soon!



# PCGenesis Server Requirements

- A **stand-alone** server. No other applications can be on the PCGenesis server.
- The **K:** mapping must be defined as a **stand-alone partition** of at least 500 GB
- The PCGenesis server **must be kept up to date** with all Windows operating system service packs applied.
- 64 GB Memory
- 1 TB Hard Drive
- **C:** 500 GB Minimum
- **K:** 500 GB Minimum

# PCGenesis Server Requirements

- Create **GENUSERS** user security group with full access (Read/Write)
- Include all PCG users in this security group
- Map **K** = **\\NewServer\PCGenesis\$**

# PCGenesis Server Requirements

- **Remote Desktop Connection (RDP)** is the **required** method for all users accessing PCGenesis.
- Better network security!
- PCGenesis processes will continue to run even if the network connection goes down
- Much faster processing
- More reliable data integrity



# PCGenesis Server Requirements

- Use a windows firewall to limit RDP connections to the PCGenesis server to only the necessary workstations.
- If school district staff require the ability to access PCGenesis externally, require them to use a Virtual Private Network (VPN), and use the firewall to assign that traffic to a specific internal subnet that can be allowed through the windows firewall on the PCGenesis server.



# PCGenesis Server Requirements

Highly recommended:

- PCGenesis be a virtual machine (VM)
- Backup solutions should include an option for "immutable backups" and that option should be enabled.
- Use Multi-Factor Authentication for RDP connections to the PCG server. This can be accomplished using Azure MFA or third-party applications.



# Agenda

- Introduction
- Backing Up PCGenesis
- PCGenesis Server Requirements
- **Ransomware Attacks**
- PCGenesis Broadcast E-mail List



# Ransomware Attacks

It's been estimated that 60% of current malicious activity is focused on Education Data.

# Ransomware Attacks

- Personally Identifiable Information (PII)
- Payroll data
- Academics
- Biometrics
- Behavioral
- Disciplinary
- Medical
- Web Browsing History
- Geolocation
- IP Addresses
- Classroom Activities
- Other Sensitive Indicators



# Ransomware Attacks

# Phishing

# Ransomware Attacks

“Email phishing shows no sign of stopping anytime soon and there is little defense to protect an endpoint where the user unknowingly cooperates with the attacker by clicking within the email.”

# Ransomware Attacks

“Phishing attacks will continue to work, and without major changes in cyber defense strategy, these attackers will continue to get in and steal your data.”

# Ransomware Attacks

- **Deceptive Phishing**

Ex: You get an email from a bank claiming that your account has been frozen unless you click on the link provided and enter your account information.

- **Spear Phishing**

Ex: You get an email that's supposedly from your organization's HR department asking you to verify your benefits policy information.

# Ransomware Attacks

- **CEO\Executive Fraud Phishing**

Ex: You get an email that's supposedly from your CEO saying they need you to wire transfer the money, and to let you know when you're free so they can send you the information of where it needs to go. (W2's)

- **Malware-Based Phishing**

Ex: You get an email from someone you don't know asking you to download an invoice.

Used to deliver viruses, worms, Trojan horses, ransomware, or other malicious programs.

# Ransomware Attacks

- Are you familiar with the sender of the email?
- Does the message contain poor grammar or misspelled words?
- Are there any suspicious links or unexpected attachments?
- Do the attachments have a strange or unexpected file extension?

# Ransomware Attacks

- Does the message make unrealistic promises like large sums of money or threats?
- Does the message plead with you or use emotional language?
- Hover over the link to ensure that the url is what you expect to see

# Ransomware Attacks

**From:** Richard Woods [<mailto:ceo@cwebb.club>]  
**Sent:** Monday, February 04, 2019 8:44 AM  
**To:** Randy Trowell  
**Subject:** DD Information

Randy,I need to update my pay check direct deposit info

Thanks  
Richard Woods

Sent from my iPhone



**From:** MS Mesaage Center <[nonrespondserver@ns1.bangkokvoice.com](mailto:nonrespondserver@ns1.bangkokvoice.com)>  
**Sent:** Monday, January 7, 2019 12:43 PM  
**To:** Louis Erste <[LErste@doe.k12.ga.us](mailto:LErste@doe.k12.ga.us)>  
**Subject:** Shutdown Request



**From Bangkok??**

This email is from a trusted source.

# Office365

Hi [lerste@doe.k12.ga.us](mailto:lerste@doe.k12.ga.us),

We received a request from you to shutdown this email account [lerste@doe.k12.ga.us](mailto:lerste@doe.k12.ga.us). This request will be processed shortly. If you did not authorize this action kindly cancel now if not disregard this message.

CANCEL

REQUEST

Thanks for taking additional steps to keep your account safe.

Regards,

Microsoft Support

This email was sent to [lerste@doe.k12.ga.us](mailto:lerste@doe.k12.ga.us).

# Ransomware Attacks

“Phishing attacks will continue to work, and without major changes in cyber defense strategy, these attackers will continue to get in and steal your data.”

## Ransomware Attacks

Attackers go for the  
low-hanging fruit:

## Ransomware Attacks

Attackers go for the  
low-hanging fruit:

**Humans**

Most Attacks Rely on Social Engineering

# Ransomware Attacks

Employees are your  
last line of defense

# Ransomware Attacks

Train, Train, Train  
Aware, Aware, Aware

This is the only way to attack the human factor and you can't do this alone. This takes a team and typically an outside resource.

# Ransomware Attacks

- **Baseline Testing**

Test to assess your users in falling for simulated phishing attacks.

- **Train Your Users**

Provide real world examples and use 3<sup>rd</sup> party content providers when possible.

- **Phish Your Users**

Use tools that have templates that mimic actual companies and accounts they are familiar with.

- **See the Results and Share**

Analyze and share stats and graphs of trainings and phishing exercises with staff and leadership.

# Ransomware Attacks

## Phishing Awareness





# Ransomware Attacks

- GaDOE has secured **KnowBe4** Diamond level licensing for every district and charter school in the state
- **KnowBe4** is the consistent industry leader in cybersecurity awareness and training
- **KnowBe4** provides the ability to do managed phishing campaigns
- Gives districts access to the **KnowBe4** library of cybersecurity training to use in your district
- GaDOE license is current through 8/31/2026

# PCGenesis

## Ransomware Attacks and Backing Up PCGenesis

# Questions?

# Agenda

- Introduction
- Backing Up PCGenesis
- PCGenesis Server Requirements
- Ransomware Attacks
- **PCGenesis Broadcast E-mail List**



# PCGenesis User List

- The Ga DOE has created an e-mail user list for PCGenesis
- This is a discussion forum
- Users can broadcast an e-mail to all PCGenesis users enrolled in the group

# PCGenesis User List

- We already have 209 registered users
- Any user involved with PCGenesis can join:
  - Financial Directors
  - Payroll Administrators
  - IT Specialists

# PCGenesis User List

Those PCGenesis districts and RESAs that join the user list will be able to:

- Share ideas
- Discuss problems
- Have many more resources available for gaining insight into PCGenesis operations

# PCGenesis User List

- Join by sending a blank e-mail to:  
**join-pcgenesis@list.doe.k12.ga.us**
- After joining, users can take advantage of discussion forums by sending e-mails to:  
**pcgenesis@list.doe.k12.ga.us**

# Future Plans

## Help us focus our efforts

- What major feature/function do you need?
- We welcome your input/requests in writing
- Complete the '**Comments and Requests**' today
- Provide your input during the discussions



# Site Recommendations

- Upgrade any server > 3 to 5 years old
- Implement **Remote Desktop** access !!!!
- Weekly full system backup of **K:\\*.\*** (Retain 3 weeks)
- Daily backups of data (**K:\SECOND** and **K:\PCGSQLDB**) to CD/DVD/USB (Retain for 1 month)
- Document restore procedures for emergencies

# PCGenesis Documentation



<http://www.gadoe.org/Technology-Services/PCGenesis/Pages/default.aspx>

# PCGenesis Documentation

 → Technology Services → Technology Services → PCGenesis

## PCGenesis

Financial Accounting and Reporting System Operations Guide

Payroll System Operations Guide

Personnel System Operations Guide

Certified/Classified Personnel Information (CPI) System Operations Guide

Budget System Operations Guide

LUAS Manual

Technical System Operations Guide

Release Information

## PCGenesis

---

- [Financial Accounting and Reporting System Operations Guide](#)
- [Payroll System Operations Guide](#)
- [Personnel System Operations Guide](#)
- [Certified/Classified Personnel Information \(CPI\) System Operations Guide](#)
- [Budget System Operations Guide](#)
- [LUAS Manual](#)
- [Technical System Operations Guide](#)
- [Release Information](#)

# Questions?



# Thank you for attending!

