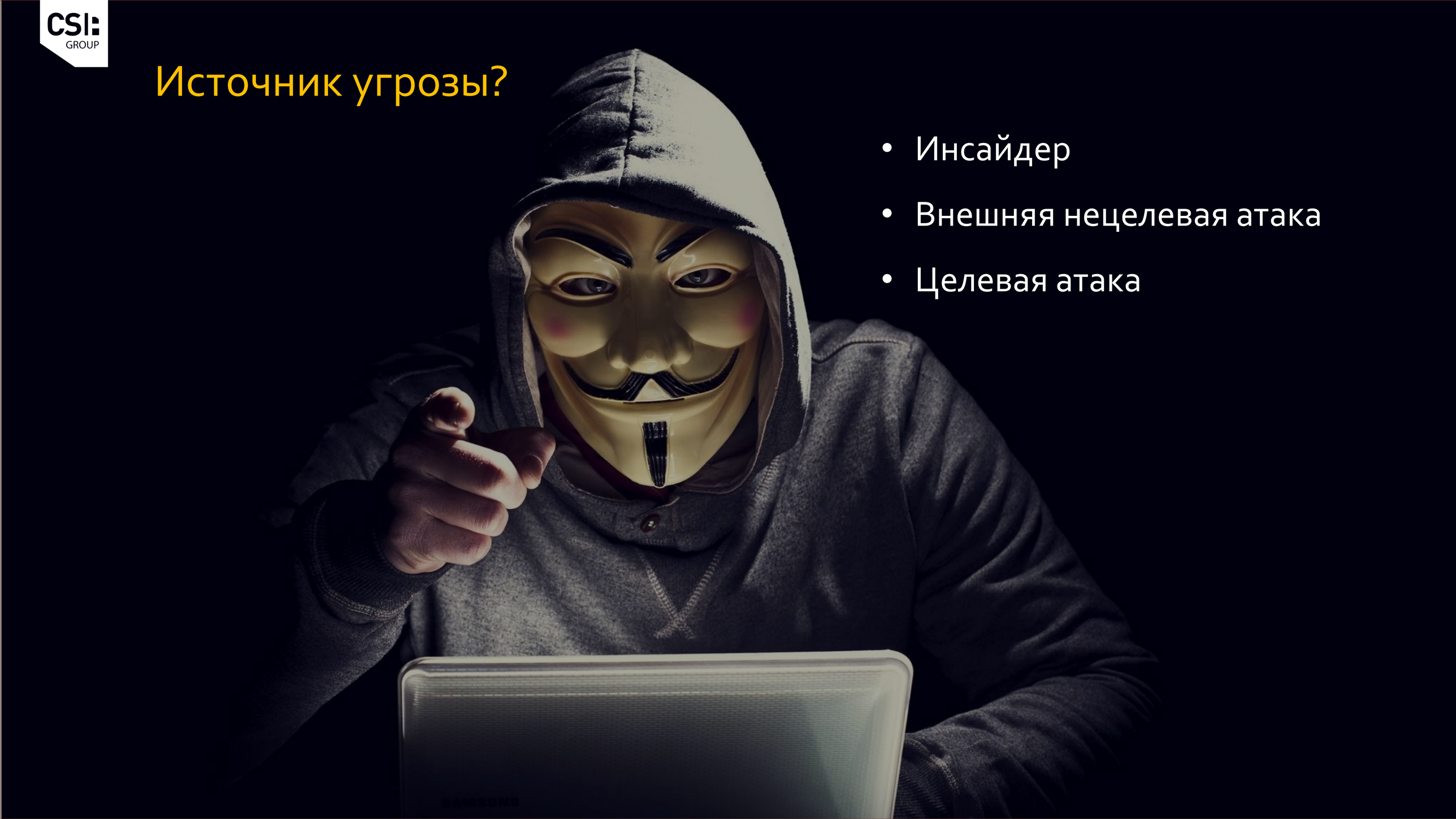
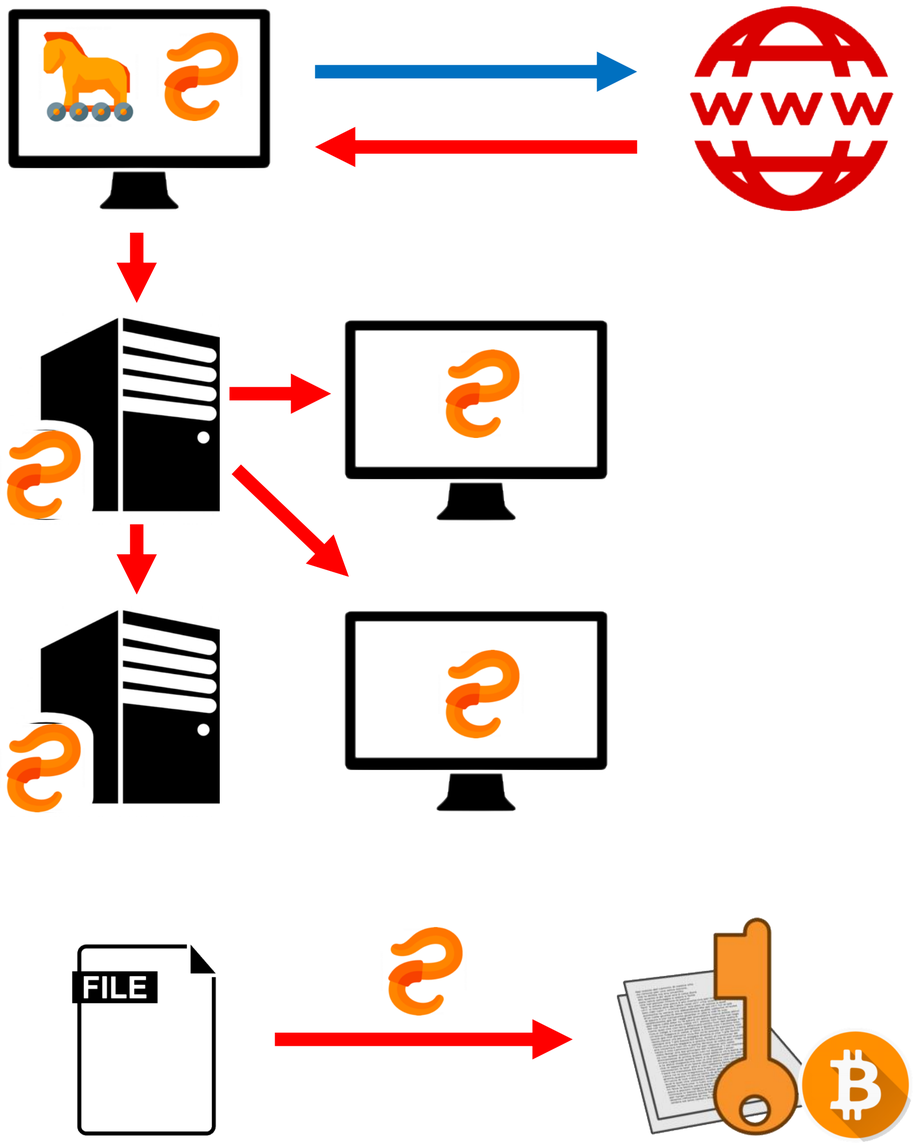

CSI
Cyber Attack
Защита чувствительной информации

Источник угрозы?



- Инсайдер
- Внешняя нецелевая атака
- Целевая атака

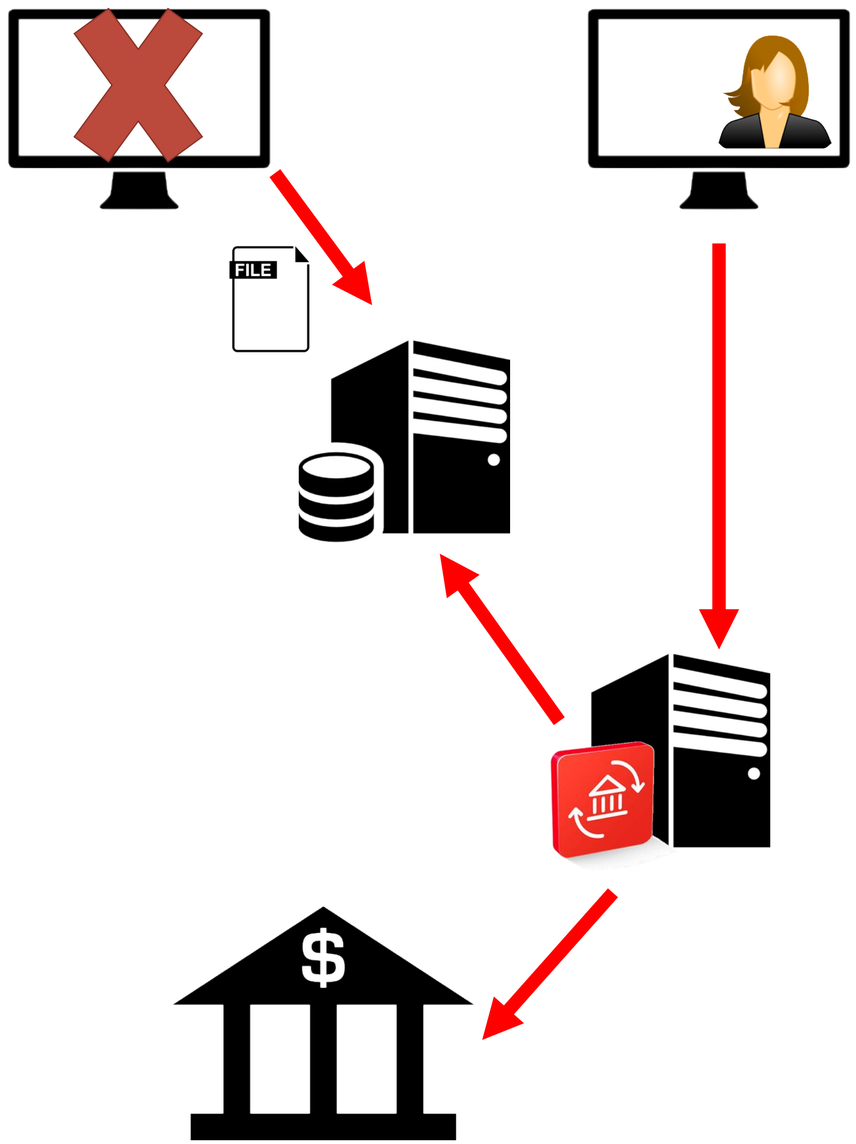


Case study 1:
Crypto

ТОП 10 операторов рекламы в РФ
23 Января 2018г – пропадает доступ к базам 1С и корпоративным документам
Остановлены сдача отчетности, расчеты с контр-агентами, платежи …

Результаты исследования:

- Использованы уже закрытые вендорами уязвимости;
- Все компьютеры и серверы имеют установленный антивирус;
- Отсутствие разграничения прав доступа к сетевым ресурсам;
- Пользователи работают с правами администратора;
- Отсутствует полноценное бэкапирование;
- Не производится мониторинг событий



Case study 2:
Ghost

ТОП 20 страховых компаний в РФ
29 Декабря уходят в оплату платежные поручения на сумму 65М рублей
Сотрудник, чья учетная запись использовалась, в отпуске с 11 Декабря

Результаты исследования:

- Аудит доступа к сетевому диску не ведётся;
- Доступ к сетевому диску имеет 65 человек;
- Компьютер основного подозреваемого исчез;
- Пароли от учетных записей не хранятся в секрете;
- Отсутствует механизм верификации платежей непосредственно перед оплатой;

Слабые места в защите конфиденциальной информации

- Незакрытые общеизвестные уязвимости
- Небезопасные конфигурации оборудования и программного обеспечения
- Слабое управление учетными записями и правами доступа
- Отсутствие процессов реагирования на инциденты и восстановления после сбоев

CSI GROUP

Critical Security Controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Наш взгляд на эффективную защиту информации

Персональные компьютеры

- Шифрование содержимого жестких дисков
- Двухфакторная аутентификация
- Минимальный набор ПО и контроль за его обновлением
- Антивирус + Host IPS
- Ограничение доступа к съёмным носителям
- Использование внешних носителей с аппаратным шифрованием
- Резервное копирование критичных данных
- DLP (опционально)

Наш взгляд на эффективную защиту информации

Сетевая инфраструктура

- Шифрование трафика и данных на серверах
- Строгая аутентификация пользователей и устройств для доступа к сети
- Разграничение прав доступа в соответствии с принципом минимизации привилегий
- Логирование действий пользователей
- Минимальный набор ПО, сервисов и контроль за их обновлением
- Доменная архитектура
- Фильтрация трафика по протоколам и портам
- Резервирование серверов и критичных

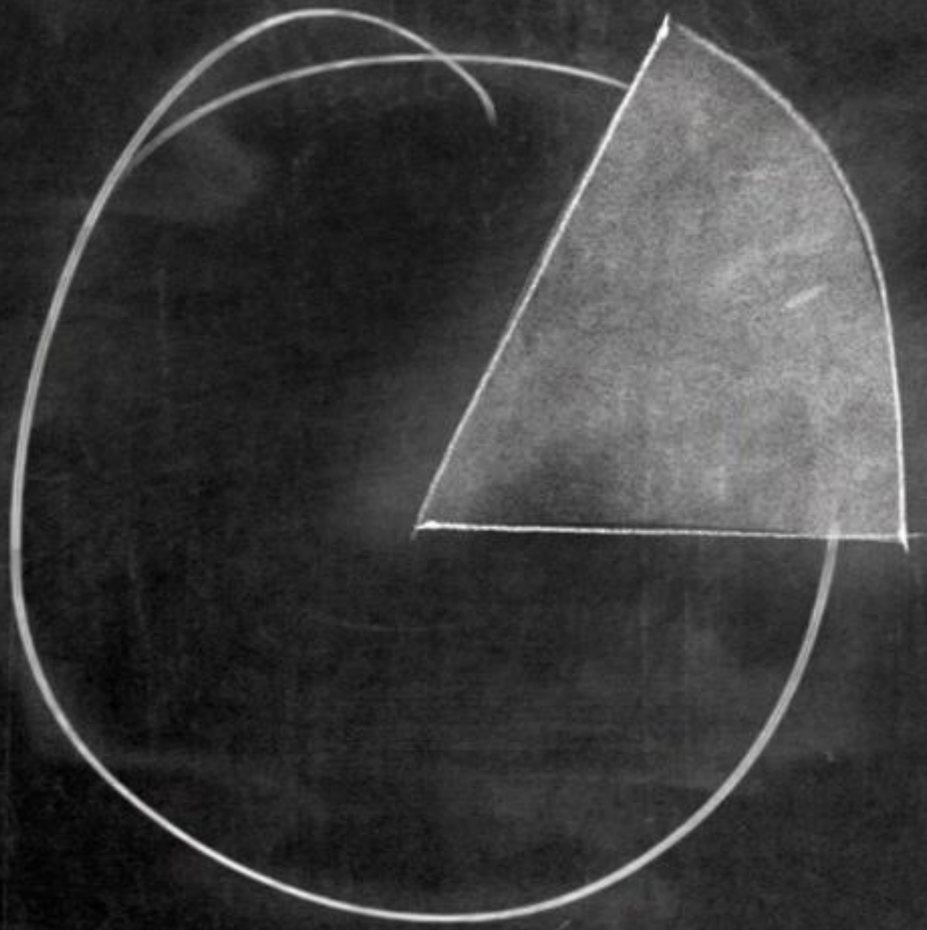
Наш взгляд на эффективную защиту информации

Мобильные устройства и частная коммуникация

- iPhone 5s или новее с последним обновлением
- Android с включенным шифрованием памяти и последним обновлением
- Буквенно-цифровой пароль на разблокировку
- Мессенджеры с паролем на разблокировку и сквозным шифрованием
- Разделение учетных записей/устройств для личной и рабочей переписки
- Использование зарубежных почтовых сервисов
- Шифрование конфиденциальных вложений
- Использование двухфакторной аутентификации везде, где это возможно
- Использование VPN

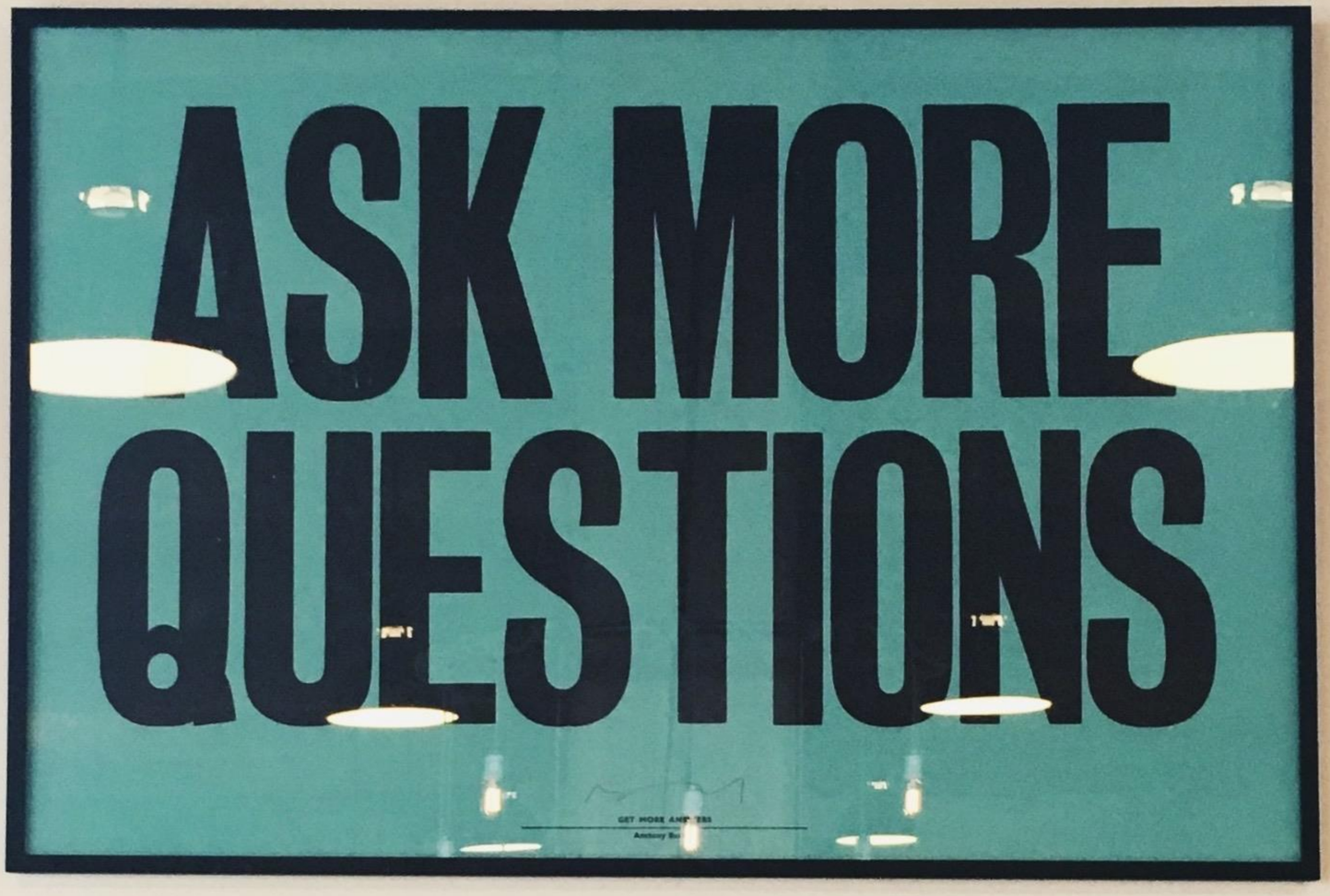
CSI GROUP

THE RULE OF 80/20



20%

FOCUS HERE!



Alexander Pisemskiy
Executive Director

Email: ap@csi.group

www.csi.group